Project acronym:	PRESCIENT
Project title:	Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment
Project number:	244779
Programme:	Seventh Framework Programme for research and technological development
Objective:	SiS-2009-1.1.2.1: Privacy and emerging fields of science and technology: ethical, social and legal aspects.
Contract type:	Collaborative project
Start date of project:	1 January 2010
Duration:	36 months

Deliverable 2:
Privacy, data protection and ethical issues in new and emerging technologies: Five case studies

Editors:	Rachel Finn and David Wright, Trilateral Research & Consulting
Authors:	Rachel Finn, Michael Friedewald, Raphael Gellert, Serge Gutwirth, Bärbel Hüsing, Piret Kukk, Emilio Mordini, Philip Schütz, Silvia Venier, David Wright
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	30 September 2011
Submission date:	25 November 2011

Terms of use

Table of Contents

Chapter 1, Introduction: Privacy, data protection and ethical issues in new and emerging technologies

Rachel Finn and David Wright
Trilateral Research & Consulting, LLP

1.1 INTRODUCTION

The first PRESCIENT deliverable examined the legal, social, economic and ethical conceptualisations of privacy and data protection. It discussed these two legal concepts and explored how they might be balanced against other values or rights such as security. The report also made general suggestions about how both privacy and data protection might be challenged by new and emerging technologies, particularly in relation to ICT and surveillance technologies. This report develops these ideas further through the use of five different case studies to specifically examine how general ideas around the relationship between new technologies, privacy and data protection can be translated into specific examples.

The purpose of this report is to describe five case studies involving different emerging technologies expected to have significant impact on privacy in order to consider how well current legal and other regulatory mechanisms are suited to address the privacy and ethical issues raised by these technologies. This report identifies and analyses privacy, data protection and ethical issues raised by the following emerging and technologies: RFID enabled travel cards and passports, "new surveillance technologies", such as whole body imaging scanners and unmanned aircraft systems, second generation biometrics, whole genome sequencing and human enhancement. For each technology the authors also identify uncertainties in the legal environment as a result of new and emerging technologies. These uncertainties are brought together to yield insights on how our understanding of privacy and data protection may change in the light of those technologies, and to assess how privacy and data protection are weighed against other ethical and social values, particularly human dignity, equality and the rule of law[1]. By these terms, but most especially the "rule of law" we mean protections surrounding free will, freedom from discrimination, freedom to travel, rights to security and rights of self-determination.

1.2 METHODOLOGY

In order to provide a full picture of the potential privacy impacts and the adequacy of current regulatory mechanisms each of the case studies analyses six issues: (1) the current status-quo of the technology, including (where relevant) its capabilities and applications, and the expected progress in the near future; (2) the set of academic, and industrial actors that are driving the development of this technology, and their intentions; (3) possible users or beneficiaries of the technology; (4) possibilities for privacy-infringing or ethically problematic uses and practices; (5) the extent to which existing ethical principles and legal regulations are valid and applicable for the technology; (6) possible pathways for future oriented new ethical rules and regulations to ensure the right to privacy. Given the European context in which this report is written, we focus upon the European legal and policy framework, however, in many cases we also refer to practices and laws in third countries.[2]

1.3 OUTLINE OF THE REPORT

We have two RFID case studies in two separate chapters. The first examines the use of RFID-enabled travel cards in public transport. It examines the widespread deployment of these

[1] Székely, Ivan, Máté Dániel Szabó and Beatrix Vissy, "Regulating the future? Law, ethics, and emerging technologies", *Journal of Information, Communication & Ethics in Society*, Vol. 9, No. 3, 2011, pp. 180-194.
[2] The focus of the research is based on western values and norms given our focus on the EU.

travel cards to assist customers, industry, transportation companies, local authorities, police and security services to benefit from increased efficiency and less congestion in public transport as well as the information collection capabilities that enable refunding, online or mobile top-ups to credit and theft protection. However, these benefits come with certain, specific risks to privacy, both through the exploitation of insecurities in cards, chips and back-end systems and the misuse of personal information. Specific risks to privacy include the unauthorised reading or use of personal information, the use of RFID information to track or pinpoint an individual's location and the unauthorised use of personal information in relation to marketing. The chapter examines the relationship between these privacy issues and different regulatory mechanisms such as privacy enhancing technologies, industry or corporate standards, data protection legislation in different Member States or third countries and European legislation. The chapter concludes that the European Commission and Member States should work proactively to ensure that transport passengers' personal information is protected from unwanted compromise, by introducing

- privacy-enhancing technologies into the systems themselves,
- processes such as privacy impact assessments and
- laws and regulations which make these measures legally binding.

The second case study (Chapter 3) examines the introduction of RFID-enabled passports, or e-passports, in the last 10 years. The case study begins by discussing RFID technologies as systems, comprising chips, readers, middle ware and back-end systems. It introduces and contextualises the introduction of RFID-enabled passports in response to events in late 2001. It continues by identifying the stakeholders involved in the introduction of RFID-enabled passports and their relative positions, including government stakeholders, international organisations, industry players, non-government organisations and end users. The next section outlines some potential privacy-infringing issues in relation to RFID-enabled passports. These include issues surrounding the security of the chips and back end systems, data processing operations which threaten privacy, such as unauthorised reading or clandestine tracking, and the specific privacy violations that could arise from these data processing operations. This is followed by a discussion of the ways in which both the e-Privacy Directive and the Data Protection Directive may address these privacy concerns. The chapter concludes with recommendations surrounding future-oriented regulatory instruments that could address some of the privacy infringements not currently considered under existing legislation. These include, for example, issues such as consent, the right to be informed of how data is being processed and rights of access. The chapter argues that technical solutions such as privacy by design or privacy impact assessments could address some of the potentials for privacy infringement. However, there is a clear need for technology-specific, tailor-made legislation.

Chapter 4 seeks to identify the ethical, privacy and data protection concerns surrounding the use of "new surveillance technologies" in Europe. The report focuses on two case studies, whole body imaging scanners and unmanned aircraft systems (UASs), both of which have newly emerging civil applications. Hundreds of whole body imaging scanners are currently deployed in airports in the USA, Europe, Canada, Nigeria and Russia, while other countries are conducting trials or considering their use. Significantly, this deployment of whole body scanners has raised controversy around the world in relation to privacy, data protection and ethics and a range of different regulatory mechanisms, including legislation, codes of practice, privacy by design enhancements and industry standards have been used to attempt to mitigate privacy concerns. In contrast, the use of UASs (more commonly known as "drones") has generated significantly less debate around privacy and data protection, despite a slow increase in the introduction of UASs in civil applications, such as law enforcement, border patrol and

other regulatory surveillance. This report analyses the current deployments of these technologies and the stakeholders who are involved, and explores the ethical, privacy and data protection issues that these technologies raise. It also examines whether existing ethical principles and legal regulations are valid and applicable for these technologies and what sorts of rules should be implemented in the future to ensure the right to privacy.

Chapter 5 focuses on "second generation biometrics". The chapter discusses key elements of these technical developments, including the emergence of new biometric traits (the so-called *behavioural*, *physiological* and *soft* biometrics) and the ways in which they are often used in combination with more traditional traits in multiple biometrics or multimodal systems, as well as the shift to embedded systems, where biometric technologies can support the wider trends towards ambient intelligence or ubiquitous computing. The chapter argues that such "next generation" biometrics are giving rise to a new set of ethical, legal and socio-political issues that have not yet been discussed in depth. In order to fully examine emerging ethical, legal and socio-political issues, this chapter outlines the primary drivers and barriers for their deployment and the current and potential applications of traditional and future biometrics in Europe. The second part of the chapter elaborates on the ethical and privacy impacts of second generation biometrics and describes possible options for the future governance of these biometric systems.

Chapter 6 focuses on whole genome DNA sequencing. This case study examines the recent history of DNA sequencing and identifies emerging applications, such as the high throughput uses of DNA sequencing in research, the Personal Genome Project (a large, publicly accessible database of 100,000 voluntary entries) and the expansion of the use of DNA sequencing in forensics. The chapter continues by discussing the relationship between the different stakeholders interested in or affected by changes in DNA sequencing as well as their respective positions. It discusses the privacy impacts of whole DNA sequencing in relation to potential privacy infringements in different contexts such as research, biobanking, direct-to-consumer testing, paternity or familial relationships and forensics. Finally, it examines the applicability of the Prüm Treaty to the use of whole DNA sequencing and makes recommendations regarding regulatory mechanisms needed to address the privacy concerns identified. Some general recommendations include harmonising legislation across different EU Member States and making codes of practice legally binding. The chapter also argues that it should be a common aim to develop and publish a concise, accurate and easy-to-understand, information policy for each of the applications of DNA sequencing, including considerations of ethical concerns such as appropriate informed consent and viable alternatives. Further recommendations are organised by context and discuss recommendations in relation to research, biobanking, forensics and direct-to-consumer testing.

Chapter 7 focuses on human enhancement. This chapter begins with a discussion on the complexity inherent in attempting to define "human enhancement"; however, it identifies three key attributes of the concept, namely artificial (socially controversial), internal (within the human body) and non-therapeutic (no medical application). Since technological and pharmaceutical forms of enhancement reflect the main fields of applications, the chapter discusses brain computer interfaces (BCIs) and neuro-enhancing pharmaceuticals as representative cases. After outlining the functionality of BCI technology and specific pharmaceutical neuro-enhancers, the chapter introduces the most important stakeholders shaping future developments in these fields of enhancement. Next, the chapter outlines the implications for data protection and privacy. It argues that whereas BCI technology heavily affects data protection because the gathered data of brain activity contains highly sensitive personal information with

an unprecedented quality and depth, pharmaceutical neuro-enhancers and implanted BCI technology pose a risk to the concept of bodily privacy and personal autonomy. The case study concludes that privacy in the context of human enhancement (if it comprises personal choice) should be regarded as a context-dependent and subjective notion, and should be reconciled with the other values and goals of the user. However, when it comes to data protection, BCI technology seems to be heavily under-regulated.

Chapter 8 identifies uncertainties in the legal environment relating to each of the case studies. It focuses on privacy and data protection as a discussion of the ethical and social implications occurs in the final chapter. This chapter uses information from the case studies to assess whether and how the Charter of Fundamental Rights can serve as a basis for legislative action that would help to resolve the identified uncertainties. The chapter compares the protections contained in the European Convention on Human Rights, the Charter of Fundamental Rights and the Data Protection Directive (95/46/EC) as well as internationally accepted data protection principles with the potential for privacy infringing practices described in the case studies. It presents two conclusions. First, privacy and data protection are two different legal instruments with different contents. These two rights are not identical, and even when both are applicable, they do not necessarily equate with one another. Second, it argues that the extent of the processing is an important consideration. Instead of trying to minimise the processing of personal data, the new technologies discussed here seem instead to nurture a maximal processing of data.

Finally, a synthesis chapter consolidates the findings from each of the case studies and presents the range of different emerging and foreseeable privacy issues demonstrated by the case studies. It begins with a review of the privacy and ethical implications of each of the case study technologies and matches these to the different aspects of privacy discussed in the first PRESCIENT deliverable. It discusses how our understanding of privacy and data protection has changed in light of the case study technologies and assesses how privacy and data protection are weighed against other ethical and social values related to human dignity, equality and the rule of law. We demonstrate that the convergence of different technologies adds a new layer of complexity and uncertainty in perceiving privacy and ethical issues. Given this complexity, we argue that a flexible conception of privacy and data protection needs to be adopted by organisations seeking to regulate new and emerging technologies and that multi-dimensional regulatory mechanisms are most appropriate to minimise negative impacts on privacy, data protection and ethics, while still protecting individuals' other rights.

Chapter 2, RFID-enabled contactless cards for public transport: security, privacy, ethics and legislation

Rachel Finn and David Wright
Trilateral Research & Consulting, LLP

2.1 INTRODUCTION

As the first part of the RFID case study, this chapter examines the use of RFID-enabled travel cards on public transport. It explores the widespread deployment of these travel cards to assist customers, industry, transportation companies, local authorities and police and security services to benefit from increased efficiency and less congestion on public transport. However, these benefits come with certain, specific risks to privacy, both through the exploitation of insecurities on cards, chips and back-end systems and the misuse of personal information. Specific risks to privacy include the unauthorised reading or use of personal information, the use of RFID information to track or pinpoint an individual's location and the unauthorised use of personal information in relation to marketing. This chapter examines the relationship between these privacy issues and different regulatory mechanisms, such as privacy enhancing technologies, industry or corporate standards, data protection legislation in different Member States or third countries and European legislation. We conclude that the European Commission and Member States should work proactively to ensure that transport passengers' personal information is protected from unwanted compromise, both through introducing privacy-enhancing technologies into the systems themselves, through introducing processes such as privacy impact assessments and through introducing laws and regulations which make these measures legally binding.

2.2 CURRENT STATUS OF RFID-ENABLED TRAVEL CARDS AND EXPECTED PROGRESS IN THE NEAR FUTURE

Radio Frequency Identification (RFID) enabled cards for use on public transportation were first introduced in the mid-1990s. The initial purpose of the cards was to reduce congestion in transportation systems, especially at peak times, by speeding up the ticketing process, and reduce fare evasion by ensuring that access to transportation systems is only available to those who have paid the proper fare. Konomi and Roussos, writing about the introduction of RFID-enabled Oyster Cards in London, note that:

> until the early 1980s commuters had to pay separately for each mode of transport that they used as the bus network, the Tube and commuter railways employed separate systems. This situation inevitably produced considerable inconvenience… [and] significant delays.[3]

RFID-enabled contactless systems rely on silicon chips and antennas embedded in plastic cards that transmit the information on the chip to a receiver, such as that installed at a ticket barrier. The electromagnetic charge generated by a receiver enables the chip in the card to transmit information, such as information about a season pass, a weekly pass and/or the amount of credit carried on the card. Each chip has a unique identification number, and details of where the card has been swiped or tapped are fed to a central database. In this way, passengers can enter an identification number and view their journey details over a set period of time.[4] The unique identification code also enables individual cards to "be singularly recognized and...hotlisted" so that individuals attempting to use lost, stolen or fraudulent cards can be prevented from using the system.[5]

---

[3] Konomi, Shin'ichi and George Roussos, "Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments", *Perspectives on Ubiquitous Computing*, Vol. 11, 2007, p. 508.

[4] "Oyster data use rises in crime clampdown", *The Guardian*, 13 March 2006. http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation

[5] Konomi and Roussos, 2007, p. 511.

Most RFID-enabled smart cards in Europe use either the MiFare chip or the Calypso chip, both of which conform to ISO 14443 standards. Other areas, such as Dublin and the North Rhine-Westphalia region, have sourced their own chips, most of which are also ISO 14443 compatible.[6] Chips which are ISO 14443 compatible operate at 13.35 MHz, which corresponds to a read range of approximately 10 centimetres.[7] This means that the cards, and the chip inside, must be relatively close to an authorised reader in order for the information to be "read" from the chip. According to Konomi and Roussos, "the range of the system was restricted to only a few centimetres", because "it must always be clear which card is presented to which gate by which passenger to ensure that correct charges are applied" particularly in locations where "a large number of individuals [are] using the system concurrently and at close proximity to each other".[8] RFID-enabled smart cards are part of a large ticketing system that includes cards, readers, communication infrastructure, databases and computing hardware. The systemic nature of these transportation systems was evidenced in one high profile failure in the London Oyster Card system, where in 2008 a software "glitch wiped as many as 40,000 cards".[9]

Some of the largest deployments of RFID-enabled travel cards include Transport for London's Oyster card system (used daily by more than 5 million commuters[10]), the OV-chipkaart ("Europe's first nation-wide multi modal public transport card"[11]) and the Octopus Card in Hong Kong ("used by nearly 95% of residents"[12]). RFID-enabled travel card projects exist or are underway in Europe, North America, South America, Asia and Australia, and although examples are too numerous to list here, Cubic Transportation Systems, one of the major suppliers of contactless smart card systems, claims the following range of customers:

> Cubic has delivered over 400 projects in 40 major markets on five continents. Active projects include London; Brisbane (Southeast Queensland) region, Australia; New York / New Jersey region; Washington, D.C. / Baltimore / Virginia region; Los Angeles region; San Diego region; San Francisco region; Minneapolis/St. Paul; Chicago; Atlanta region; Miami (South Florida) region; Vancouver and Edmonton, Canada; Sydney (New South Wales), Australia; and Scandinavia.[13]

This gives some indication of the popularity of such smart card systems in transport. Calypso Networks Association, which implemented the original Paris Navigo Card in 1995, claims to be operating in 21 countries and 80 different urban markets, including Montreal, Brussels, Lisbon, San Paulo and Skopje.[14] Another major system company, Octopus Card Limited, op-

---

[6] Railway Procurement Agency, "ITS FAQs", 2008. http://www.rpa.ie/en/its/Pages/ITSFAqs.aspx#anchor_use

[7] ASK, "Contactless Technology", 2011. http://www.ask-rfid.com/Technology/Contactless/tabid/101/language/en-US/Default.aspx

[8] Konomi and Roussos, 2007, p. 510-11.

[9] Thompson, Iain, "Oyster card system clams up; Glitch wipes 40,000 cards", vnunet.com, 15 Jul 2008. http://www.v3.co.uk/vnunet/news/2221591/oyster-card-system-clams

[10] Konomi and Roussos, 2007.

[11] van't Hof, Christian, and Jessica Cornelissen, *RFID and Identity Management in Everyday Life: Case Studies on the Frontline of Developments towards Ambient Intelligence*, European Technology Assessment Group, Oct 2006, p.10.

[12] Octopus Holdings Limited, "Corporate Profile: Hong Kong Services", 2009. http://www.octopus.com.hk/about-us/corporate-profile/services-in-hong-kong/en/index.html

[13] Cubic Transportation Systems, "Cubic Signs $220 Million Contract to Design, Build, Operate and Maintain Vancouver Smart Card and Faregate System", press release, 27 Jan 2011. http://cts.cubic.com/AboutUs/News/News/tabid/434/articleType/ArticleView/articleId/30/language/en-GB/Cubic-Signs-220-Million-Contract-to-Design-Build-Operate-and-Maintain-Vancouver-Smart-Card-and-Faregate-System.aspx

[14] Calypso Networks Association, "Implementations", 2011. http://www.calypsonet-asso.org/index.php?rubrique=main_50

erates in the Netherlands, Hong Kong, Dubai and New Zealand. Other examples include the Monedero Card in Buenos Aries and the Travel Card in New Delhi.

One of the key ways in which the RFID travel card market is seeking to expand and evolve is through the use of Near Field Communication (NFC). Technology specialists have already argued that RFID technology and NFC are often confused, where "NFC is a short-range wireless connectivity technology standard designed for simple communications between electronic devices. NFC communication is enabled by bringing two NFC compatible devices within a few centimeters of one another… [and] NFC devices share the basic technology with proximity (13.56 MHz) RFID tags and contactless smart cards, but have also specific features."[15] The primary distinction between RFID-enabled cards and NFC devices is that NFC devices must have their own processing capabilities, whereas the chips in RFID cards are passive. In relation to contactless smart cards, NFC is being utilised in two distinct ways, integrating travel and small payment capabilities into the RFID contactless card or using mobile phones as NFC devices to pay for travel and small items.

The integration of contactless smart cards for travel and debit payments has been long-promised, but has taken some time to gain public acceptance. This technology was also rolled out in the mid-1990s in the USA in relation to the Exxon-Mobile Speedpass®, which was intended for gasoline and other small purchases in Exxon-Mobile petrol stations only. Transport for London and Barclay Card have been pushing the development of the OnePulse Card – an all-in-one card that integrates an Oyster card function as well as a debit and credit function.[16] In Los Angeles, the TAP® card is being expanded to enable holders to use the card to pay for parking, events, hotels and retail purchases,[17] while officials in Venice have plans for "extended use of the cards for accessing museums, paying restaurants [and] booking concerts" to offer increased services for citizens and tourists.[18] However, it is in Asia where NFC smart cards have been most successfully expanded from transport to other sectors. The T-Money card in Seoul, South Korea can be used at convenience stores, vending machines, amusement parks, fast food stores, theatres, the university, municipal parking, tolls, copy machines and on the Internet.[19] In Taipei, the Easy Card can also be used at convenience stores, department stores, supermarkets and other retailers.

Some transportation providers have also teamed up with mobile phone companies to work towards integrating NFC technology and payment systems. Cubic Transportation Systems has teamed up with a number of other companies to offer NFC-enabled phone applications. For example, the LA TAP® system has implemented a phone application that enables law enforcement officials and fare inspectors to view the information on a traveller's smart card to ensure that the proper fare has been paid. Cubic asserts that "fare verification, fare payment, personal account maintenance, access control, operational management, data acquisition and mobile ticketing are among the new applications that will be available in our systems to sup-

[15] Dehousse, Franklin, and Tania Zgajewski, "RFID: New 'Killer Application' in the ICT World, New Big Brother or Both?", *Egmont Paper 30*, Academia Press, Gent, June 2009, p. 5.
[16] Cubic Transport Systems, "The World is their Oyster", *Collection Point: A bi-monthly magazine for Europe*, No. 1, Dec 2007, p. 6.
[17] Cubic Transportation Systems, "Case Study: Los Angeles TAP® Card System", 2010. http://cts.cubic.com/Customers/UnitedStates/CaseStudyLosAngeles/tabid/427/language/en-US/Default.aspx
[18] van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij, Claudio Borean, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, Office for Official Publications of the European Communities, Luxembourg, 2007, p. 219.
[19] Korea Smart Card Co., "T-Money Service", 2006. http://eng.t-money.co.kr/

port payment on mobile devices."[20] In the future, mobile phones will enable travellers to view their travel history on their mobiles, check their balance and top up the card at a time and place of their choosing, as well as allow "the phone to read and act upon information encoded in intelligent 'tags' embedded in everyday items such as timetables and posters".[21] However, present systems only allow subscribers to "download a 'virtual transit card' as an application to their phone and then use the phone as a reload terminal to add products to the card…. [A] file contains data on transit usage, such as the application tracking ID, the stored value balance and the journey history.[22]

2.3 STAKEHOLDERS (INDUSTRY, ETC.) AND DRIVERS DRIVING THE DEVELOPMENT OF RFID-ENABLED TRAVEL CARDS

The introduction of RFID-enabled contactless travel cards are driven by a range of actors. Most systems are procured by civic transportation authorities such as Transport for London (TfL), or by organisations of transportation companies working in conjunction in particular urban or regional areas.[23] However, most systems are delivered via a consortium of companies with different relative expertise. For example, TfL originally selected "Transys, a consortium of EDS, Cubic (each for 37,5%), and ICL (Fujitsi) and WS Atkins as supporting companies [...] to deliver the electronic ticketing system to London"[24], while the "owner and maintainer of [the OV-chipkaart] RFID environment is Trans Link Systems (TLS), a consortium of the five largest public transport companies in the Netherlands, representing 80% of the Dutch market"[25]. These consortia then contract out the construction of different components of the system to different companies. Again, taking London's Oyster card as an example, van Lieshout, et al. found that in the original Transys contract:

> Transys has chosen the Philips Mifare chip for use in the London's Oyster smart card project. The smart cards will be manufactured by Giesecke & Devrient, Germany and SchlumbergerSema, UK, while Cubic will be responsible for the readers, and EDS will be responsible for the central information system, the distribution and quality control of the cards.[26]

Such complex systems can lead to delays and problems as companies depend on one another for different components, because projects might include dozens of different public transport organisations, a range of different companies and local political actors.[27] To mitigate problems arising from corporate co-operation and to increase their market share, other companies offer a range of layered systems where, for example, the Korea Smart Card Co. provides:

> A range of services, including value added services, such as a mobile payment system, an e-money system and a customer web portal. They also offer front end systems including bus systems, train systems and ferry, taxi and total mobility systems. The next layer is back end systems, such as re-load systems, clearing systems, settlement systems, data warehouse and

[20] Cubic Transportation Systems, "Mobile and Contactless Payment", 2011. http://cts.cubic.com/Solutions/MobileandContactlessPayment/tabid/365/language/en-GB/Default.aspx
[21] Cubic Transport Systems, "Beyond the Gate: An engineer's-eye-view on emerging ticketing and gating solutions across Europe", *Collection Point: A bi-monthly magazine for Europe*, No. 2, March 2008, p. 13.
[22] Cubic Transport Systems, "Getting Smart in San Francisco", *Collection Point: Quarterly Magazine*, No. 3, June 2008, p. 4.
[23] van't Hof and Cornelissen, 2006.
[24] van Lieshout, et al., 2007, p. 214.
[25] van't Hof and Cornelissen, 2006, p. 11.
[26] van Lieshout, et al., 2007, p. 214.
[27] van Lieshout, et al., 2007.

bus management systems. Finally, infrastructure such as infrastructure/architecture, card issuance systems and monitoring systems.[28]

In a similar fashion, the 2010 transfer of the Oyster system from Transys to Cubic Transportation Systems[29] would not have been possible without the fact that Cubic now offers back-end systems via their Nextfare® Solution Suite, an open software and hardware platform that integrates "an enterprise management system and customer devices for smart card issuing, processing and validating".[30] In addition to Cubic Transportation Systems, other companies who drive the introduction of systems include vendors such as Octopus, ASK, and Calypso.

Place	Card name	Entities/companies involved	Specific uses
North-Rhine-Westphalia, Germany	VRR/VRS	VRR and VRS; T-Systems International GmbH, the IT services and infrastructure arm of German telco Deutsche Telekom AG; German Mass Transit Authority (VDV).	Trains and buses in the region.
The Netherlands	OV-chip-kaart	Octopus Holdings Limited; Dutch Railways; Philips (MiFare)	All public transport in The Netherlands.
London	Oyster Card	Cubic Transportation Systems; Transport for London; Philips;	Subway, buses, ferries and limited use on commuter rail.
Paris	Passe Navigo	Régie Autonome des Transports Parisiens (RATP); Calypso; ASK	For use on the subway, buses, trams and bicycle rental.
Dublin	N/A	Luas, Dublin Bus and Iarnród Eireann (Irish Rail); Veolia Transport Ireland; Integrated Transport Service; Hewlett Packard	Light rail, buses and commuter rail, although the cards are not integrated.
Los Angeles	TAP Card	Cubic Transportation Systems	Usable on LA metro, soon to include parking, events, hotels and retail.
Seoul	T-money card	Korea Smart Card Co.	Usable on public transport and at convenience stores. They will also be expanding this service to smart phones.
Taipei	Easy Card	EasyCard Corporation	National transport tickets, convenience stores, department stores, supermarkets, and other retailers across Taiwan.
Tokyo	SUICa (Super Urban Intelligent Card)	Sony's FeliCa (Felicity Card) technology; East Japan Railway Company	For use on train lines in Japan as well as retail purchases.
Hong Kong	Octopus Card	Octopus Holdings Limited; Sony	For use on transportation and parking, at retail outlets, self-service machines, leisure. fa-

[28] KSCC, "Korea Smart Card Co., Ltd.", 2006. http://eng.t-money.co.kr/ [Note: Some formatting in this quote has been changed.]

[29] Thompson, Rebecca, "Cubic takes on Transport for London's Oyster card IT contract", *ComputerWeekly.com*, 17Aug 2010. http://www.computerweekly.com/Articles/2010/08/17/242418/Cubic-takes-on-Transport-for-London39s-Oyster-card-IT.htm

[30] Cubic Transportation Systems, "Enterprise systems for transit", 2011. http://cts.cubic.com/Solutions/EnterpriseSystemsforTransit/tabid/363/language/en-US/Default.aspx

			cilities and schools
New Delhi	Travel Card	Delhi Metro Rail Corporation; Citibank; MiFare;	For use on the Delhi Metro, and integrated with Citibank credit card.
Buenos Aires	Monedero/ Subte card	Buenos Aires Metro (Subte)	Metro and bus lines, as well as a debit card in some small shops and in toll roads.

Table 2.1: Select examples of the use of smart cards in public transport and beyond.

Yet, while transportation systems companies drive the introduction of contactless smart card systems through sales, other corporate players drive the introduction of this technology through chip development, manufacture and outlining standards. ICT vendors such as Philips (the Mifare chip), Sony (The FeliCa chip), ASK (the C.ticket), SMicroelectronics, Infineon, Nokia and Applied Card Technologies all have a share of contracts in the contactless transport card sector. The International Organization for Standardization (ISO), Calypso and VDV have developed industry standards for the RFID chips used in contactless cards, specifically, the ISO 14443 standard

2.3.1 Beneficiaries of RFID travel cards

While there are some clear beneficiaries of RFID-enabled travel cards, public transport providers who procure the systems may paradoxically receive the least secure benefits from the system. Private companies, as well as Member States and the European economy benefit from the revenues generated for European companies in providing RFID-enabled travel cards. Commuters benefit from financial advantages from discounts available as a result of using the card[31], convenience in terms of quick entry and exit to and from transport systems, security in terms of excluding those who have not paid a fare[32] and convenience in terms of automated or Internet-based credit reload systems. Consumers also experience indirect benefits, such as more personalised services and marketing, which have been criticised as potentially privacy infringing practices. Police and security services have also benefited from the time and location data available about individual travellers as a result of RFID-enabled travel systems. The BBC and *The Guardian* have both reported that the Metropolitan Police (London) have requested journey information for individual Oyster cards as part of criminal investigations.[33] Public transportation authorities may benefit from increased passenger numbers[34], modernised systems (including increased efficiency, decreased staff costs, better overall transport system management)[35] and a reduction in fare evasion[36]. However, van Lieshout et al. note that these systems often require significant financial investment, and that a return on investment may take years to materialise. In fact, none of the cases they analysed indicated savings on these points.[37]

2.4 PRIVACY IMPACTS AND ETHICAL ISSUES RAISED BY RFID-

[31] van Lieshout, et al., 2007.
[32] GVB, "What is the OV-chipkaart", 2011. http://www.gvb.nl/english/travellers/tickets-and-fares/ov-chipkaart-travel-products/pages/what-is-the-ov-chipkaart.aspx
[33] "Oyster data use rises in crime clampdown", 2006.
[34] Cubic Transportation Systems, "Case Study: London Oyster® Card System", 2011. http://cts.cubic.com/Customers/UnitedKingdom/CaseStudyLondon/tabid/430/language/en-GB/Default.aspx
[35] van Lieshout, et al., 2007.
[36] OECD, "RFID Guidance and Reports", *OECD Digital Economy Papers*, No. 152, OECD publishing, 2008.
[37] van Lieshout, et al., 2007, p. 208

ENABLED TRAVEL CARDS

Although some assert that the unauthorised reading of RFID tags "is not a significant privacy problem as the range of most RFID tags is so small",[38] many have expressed serious concerns about the potential for privacy-infringing uses and practices in RFID-enabled applications such as contactless travel cards. Many of these privacy concerns in relation to such cards focus on the physical insecurity of the chips and the related insecurity of the personal data collected by those managing the transport/travel card systems.

Research on RFID-related privacy concerns offers a number of different categorisations of security and/or privacy threats in relation to RFID systems. The OECD has outlined three dimensions of security threats for RFID systems, including availability, integrity and confidentiality threats, with examples such as "denial of service, jamming, cloning, eavesdropping and skimming."[39] Garfinkel et al. outline a series of privacy threats associated with RFID systems in general, but which can be linked with RFID-enabled contactless travel cards. Their categorisation system contains the following threats:

- *Association threat*: The association between an individual and a tag's individual serial number, which can be clandestine or involuntary.
- *Location threat*: "First, individuals carrying unique tags can be monitored and their location revealed if the monitoring agency knows the tags associated with those individuals. Second, a tagged object's location—regardless of who (or what) is carrying it—is susceptible to unauthorized disclosure."[40]
- *Preference/value threat*: An item's tag identifies the product's manufacturer, the product type, and the item's unique identity. This can result in a value threat if the monetary value of the item, or the credit on a card is can be determined.
- *Constellation threat*: Sets of RFID tags can create a unique shadow around a person or group, allowing them to be tracked, even if individual identities are unknown.
- *Transaction threat*: When a tagged transfers from one person to another, a transaction between the individual(s) can be inferred.
- *Breadcrumb threat*: This threat is similar to an association threat; however, it involves situations where the item has been dissociated from the person, without a transfer of association to the new holder. If the transferred item is used in the commission of a crime, only the original owner is implicated, not the new owner.[41]

Many of the specific privacy concerns around the security of the cards and the personal information they store or generate are associated with one or more of these threats.

There is a range of ways in which the physical security of the RFID-enabled contactless travel card system can be compromised. As Paweł Rotter warns, threats are not only to the tags themselves, but they are systemic, including threats to the air interface and threats to readers, networks and back-end systems.[42] The OECD concurs, stating that "tags and readers are not the only components of RFID systems that require security protection. Software (middle-

[38] Alfonsi, Benjamin J., "Privacy debate centers on Radio Frequency Identification", *IEEE Security and Privacy Magazine*, Vol. 2, No. 2, March-April 2004, p. 12.
[39] OECD, *Radio Frequency Identification (RFID)*, 2008, p. 4.
[40] Garfinkel, et al., 2005, p. 38.
[41] Ibid.
[42] Rotter, Paweł, "A Framework for Assessing RFID System Security and Privacy Risks", *Pervasive Computing*, April-June 2008, pp.70-77.

ware), network and database components are also subject to information security risks."[43] In a number of well publicised cases, scientists and technology experts have discovered flaws in the security of RFID chips, where simple and/or inexpensive technological purchases can compromise card security. In one case, Dutch scientists discovered that Mifare chips in Oyster cards could be cloned using a commercial laptop, and scientists used the technique to "ride free on the Underground for a day".[44] The technique relied on scientists "scanning" a card reading unit to obtain the cryptographic key and then brushing close to individuals with cards in their pockets to "sniff" the required information from the card using a reader. Similarly, researchers in the USA demonstrated a serious security weakness in RFID-enabled Speedpass® devices, by cloning the devices and using them to obtain free petrol.[45] In October 2006, American researchers also noted that RFID-enabled credit cards were susceptible to unauthorised information exchange, where they found that the cryptographic protections in the cards intended to protect sensitive information actually transmitted the card-holder's name and other details without encryption.[46] Ramos et al. note that the equipment necessary to eavesdrop on a legitimate RFID information exchange on RFID-enabled passports is available on the Internet.[47] In some cases, the necessary technology can cost as little as US $150.[48] Yet another security flaw identified is the possibility of RFID tags being infected with viruses and/or used to infect middleware and databases.[49]

Further privacy-related concerns about contactless smart cards often revolve around the use or misuse of personal information. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada defines personal information as:

> Any recorded information about an identifiable individual. In addition to one's name, contact and biographical information, this could include information about individual preferences, transactional history, record of activities or travels, or any information derived from the above, such as a profile or score, and information about others that may be appended to an individual's file, such as about family, friends, colleagues, etc. In the context of item-level RFID tags, the linkage of any personally identifiable information with an RFID tag would render the linked data as personal information.[50]

Upon registering for a contactless travel card, three major providers of these travel cards request a range of information. For example, in order to get an OV-chipkaart, van't Hof and Cornelissen report that they were required to submit the following personal details on the application form: name, address, bank account, signature and a copy of a passport.[51] On pur-

---

[43] OECD, *Radio Frequency Identification (RFID): A Focus on Information Security and Privacy*, DSTI/ICCP/REG(2007)9/FINAL, OECD Publishing, 14 Jan 2008, p. 4.

[44] Miller, Vikki, "Oyster card: fears over Mifare security", *The Telegraph*, 21 June 2008. http://www.telegraph.co.uk/news/newstopics/politics/2168791/Oyster-card-fears-over-Mifare-security.html

[45] Garfinkel, Simson L., Ari Juels and Ravi Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", *IEEE Security & Privacy Magazine*, Vol. 3, No. 3. 2005, pp. 34-43.

[46] Ozer, Nicole A., "Rights 'Chipped' Away: RFID and Identification Documents", *Stanford Technology Law Review*, Vol. 1, Jan 2008. http://stlr.stanford.edu/pdf/ozer-rights-chipped-away.pdf. See also Dehousse and Zgajewski, 2009.

[47] Ramos, Alan, Weina Scott, William Scott, Doug Lloyd, Katherine O'Leary and Jim Waldo, "A Threat Analysis of RFID Passports: Do RFID passports make us vulnerable to identity theft?", *Communications of the ACM*, Vol. 52, No. 12, Dec 2009, pp. 38-42.

[48] Ozer, 2008, p. 5, para 10.

[49] Rieback, Melanie R., Bruno Crispo and Andrew S. Tanenbaum, "Is your cat infected with a computer virus?", *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, 2006, pp. 169–179.

[50] Cavoukian, Ann, *Privacy by Design: Take the Challenge*, Information and Privacy Commissioner of Ontario Canada, Toronto, March 2009, p. 150.

[51] van't Hof and Cornelissen, 2006, p. 11.

chasing an Oyster card, the following personal details must be supplied: name, address, phone number and e-mail address.[52] Finally, according to Octopus in Hong Kong, the following personal details are necessary "to enable the elderly and students to enjoy the concessionary fares offered by different public transport service providers": name, date of birth and ID card number.[53] Most companies say that the purpose of providing personal information is to enable direct debiting, to protect the balance on the card in case it is lost or stolen and to process refunds and other procedures. Acceptance of the terms and conditions, including the use of personal data for commercial purposes, is often indicated through a customer's first use of the card.[54] However, some companies also enable individuals to purchase anonymous cards. Octopus claims that 80 per cent of their current customer base is using anonymous cards.[55] Van't Hof and Cornelissen also find that VRR/VRS in Germany explicitly claim that the RFID chips on their smart cards only store data that is relevant and necessary for the validity of the card: name, date(s) of validity-date and zone(s) of validity. They also state that no additional travel or personal details are stored, and customers can choose whether to use a personalised credit card or an anonymous debit card as payment.[56] Anonymous Oyster cards can be purchased with cash; however, they cannot be linked with season passes or discounts, as is also the case for OV-chipkaarts in the Netherlands, where anonymous cards were initially more expensive than those which collected personal information.[57] This prevention or discouragement of anonymity is central to some of the potential privacy infringing practices that civil liberties groups, technology experts, governments and academics discuss in relation to RFID embedded travel cards.[58]

A second key potentially privacy-infringing practice, and perhaps the most immediate for customers, is the potential to use the data from travel cards to pinpoint individuals' locations or to track their movements as they use public transport. The OECD argues that:

> After the fact tracking can result from bringing together location, time and other information previously stored in one or several databases, thus acting as "digital footprints".... Subway RFID cards like the Parisian Navigo Pass, the London Oyster Card or the Tokyo Suica Card allow only individuals who have paid the fee to enter in the transportation system and take the journey they have paid for. All these RFID systems need to process location information in order to perform their access control feature but if such information is stored and can be linked to the individual, it could then be used for broader tracking purposes.[59]

This location threat can be translated into a breadcrumb threat, where as Langheinrich argues, "once a specific tag or a set of tags can be associated with a particular person, the mere presence of this tag in a particular reader field already implies a (most likely unwanted) location disclosure."[60] Langheinrich points out that the association between the individual and the tag can be spurious (e.g., if the card is stolen or given to another person); however, this association is difficult to break once it is made. This generalised threat can and has materialised into specific threats. The OECD has found that passengers' latest entry and exit stations from

---

[52] Ibid.
[53] However, Octopus will stop recording customers' ID numbers in the fourth quarter of 2010. Octopus Holdings Limited, "Customer Data Protection", 2009.
http://www.octopus.com.hk/customer-service/faq/en/index.html#Service05
[54] van't Hof and Cornelissen, 2006.
[55] Octopus Holdings Limited, "Customer Data Protection", 2009.
[56] Ibid.
[57] van't Hof and Cornelissen, 2006.
[58] Garfinkel, et al., 2005, pp. 34-43.
[59] OECD, "RFID Guidance and Reports", 2008, p. 54-55.
[60] Langheinrich, Marc, "A survey of RFID privacy approaches", *Personal and* Ubiquitous Computing, Vol. 13, No. 6, 2009, p. 414.

Japanese public transport systems are stored on the Suica card and can be read by basic, commercially available RFID readers, which could facilitate stalking.[61] British newspapers have also found that the data stored in relation to the London Oyster Card is available online to anyone with the card's serial number, or who takes the card to a payment station. This data has been used in divorce proceedings as evidence of infidelity.[62] In many cities, police use data generated by travel cards as part of police investigations.[63] However, in most places, police must provide a search warrant or court order in order to be given access to the data.[64]

The unknown compromise of personal information stored in RFID chips is also a key privacy concern. Langheinrich states that one of the main privacy relevant facets of RFID technologies is that "function[s] can be accessed without a line-of-sight, i.e., both reader and tag can be completely hidden from view, making it difficult, if not impossible for the owners of scanned objects to be aware of such a process taking place".[65] The OECD also concurs, stating that the "core characteristic" of RFID is the fact that "invisible electromagnetic communications that make the collection of information by RFID devices not obvious to the person carrying the tagged product or object".[66] This data can be compromised through practices such as "skimming", where unauthorised readers can access information on the card, or through a compromise in the data security in back-end systems. Van't Hof and Cornelissen offer a specific example of back-end data insecurity, when they purchased and attempted to use an OV-chipkaart:

> A bus driver, helping [the researcher] out on many of these events, called her one night at home to inquire if everything was sorted out with the card. This account demonstrates the link between the card and the personal information in the database has not been sufficiently secured yet.[67]

Although this relates to an early deployment of interoperable RFID-enabled travel cards for use on trains *and* buses in the Netherlands, as the authors argue, the lack of security of personal data is startling.

The threat of association in relation to contactless travel cards primarily comes from the use of personal data for marketing purposes. As Srivastava argues, the aggregation of personal data can lead to companies constructing sophisticated consumer profiles.[68] This is especially true if contactless travel cards are expanded for use as payment for other small items. Van't Hof and Cornelissen found that the Dutch Railways have been "open" about their intention to use data from the OV-chipkaarts for marketing purposes, although the railway company does not specify what type of marketing.[69] As we will see below, this was a key issue that prompted the Dutch government to intervene. Langheinrich discusses Westin's definition of privacy as "'the claim of individuals… to determine for themselves when, how, and to what

[61] OECD, "RFID Guidance and Reports", 2008, p. 42.
[62] Bloomfield, Steve, "How an Oyster Card can Ruin your Marriage", *The Independent on Sunday*, 19 Feb 2006. http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html
[63] "Oyster data use rises in crime clampdown", *The Guardian*, 13 Mar 2006 and Octopus Holdings Limited, "Customer Data Protection", 2009.
[64] Octopus Holdings Limited, "Customer Data Protection", 2009.
[65] Langheinrich, 2009, p. 413.
[66] OECD, "RFID Guidance and Reports", 2008, p. 4.
[67] van't Hof and Cornelissen, 2006, p. 11.
[68] Srivastava, Lara, "Radio frequency identification: ubiquity for humanity", *info*, Vol. 9, No. 1, 2007, pp. 4-14.
[69] van't Hof and Cornelissen, 2006.

extent information about them is communicated to others'" and states that this control over personal information is violated by "sniffing" RFID tags or using them to track individuals.[70]

The use of RFID chips generally, as well as the privacy concerns surrounding RFID-enabled travel cards specifically, has prompted a range of actors to resist the use of personal information in these ways. Privacy watch groups such as FoeBud (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs) in Germany and CASPIAN (Consumers Against Supermarket Privacy invasion and Numbering) in the USA have organised public protests against the use of RFID in retail environments.[71] Van't Hof and Cornelissen found very few cases in which the use of RFID-enabled travel cards have encouraged privacy debates; however, they did find that FoeBud warned potential users on its website that the data generated by travel cards could be used to monitor people's movements and that their data could be used for other purposes.[72] It is worth noting that the VRR/VRS cards do not carry any personal data except users' names. In relation to OV-chipkaarts, which were not initially anonymous, the Dutch Data Protection Authority warned the Dutch Railways that "their storage and use of travel information was not always legitimate" and that "the aggregation of data has to be limited to the necessary data – in this case data for administering payments and not for marketing – and data can only be used once the person involved has agreed explicitly".[73] Dutch Railways states that cards can now be purchased anonymously, which would enable individuals to limit the use of their personal data. In response, some individual travellers are resisting the collection and use of their personal details in unique ways, for example by exchanging cards with one another.[74] On a more macro level, civil liberties campaigners and academics have also warned about the use of RFID-enabled devices in general, saying that RFID deployment should be halted until a formal technology assessment could take place.[75] At the European level, the Article 29 Data Protection Working Party (Article 29 WP) is looking at the use of RFID in various applications and issuing recommendations as to how the privacy issues related to RFID can be addressed.

2.5 EXTENT TO WHICH THE EXISTING LEGAL FRAMEWORK ADDRESSES THE PRIVACY IMPACTS

A range of ethical principles, codes of practice and legal regulations have been instituted for the control of the use and disclosure of personal information in relation to RFID embedded travel cards. These policy-related security measures may also work in conjunction with privacy-enhancing technologies (PETs), technical safeguards to ensure the security of information. Both the OECD and Garfinkel et al. argue that the proper security of RFID applications requires a combination of technical and policy controls, and that this is vital to ensure that these applications achieve public acceptability and economic benefits.[76]

Those who argue for the inclusion of PETs into RFID systems say that these PETs must be considered at the design stage of the system. For example, the OECD states that "privacy by design or embedding privacy in the design of the technology and of the systems can signifi-

[70] Westin, 1967, in Langheinrich, 2009, p. 415.
[71] van't Hof and Cornelissen, 2006, p. 5
[72] Ibid., p. 9.
[73] Ibid., p. 12.
[74] Ibid.
[75] Garfinkel, et al., 2005, pp. 34-43.
[76] OECD, *Radio Frequency Identification (RFID)*, 2008 and Garfinkel, et al., 2005.

cantly facilitate the protection of privacy and foster trust in RFID systems".[77] The Information and Privacy Commissioner of Ontario as well as the Article 29 WP suggest that systems should build in privacy protections.[78] One of the PET tools available to those who are designing these systems with privacy in mind is the encryption of information on the RFID tags, so that only authorised readers can communicate with them.[79] Langheinrich further argues that the communication channel between the tag and the reader must be secure.[80] Finally, in addition to technical privacy by design, systems should also design privacy into their information collection systems and procedures, where, for example, principles such as data minimisation and anonymisation should be applied.[81]

Although ethical issues such as informed consent and opt-in/opt-out mechanisms are part of any comprehensive privacy protection package, ethical ways of handing customer data in relation to privacy have been identified. For example, the OECD discusses the relationship between the privacy considerations inherent in paper tickets versus RFID-enabled tickets. The organisation states that "sometimes, the individual has no real choice but to accept the collection of data in order to benefit from an associated service", where the removal of the option of paper tickets means that peoples' "choice will then be reduced to either accepting the collection of personal data or not using the transportation system".[82] According to the OECD, this choice nullifies consent because of the cost to the individual for refusing information collection. Here, they demonstrate that although knowledge and consent are important ethical facets of any information collection system, they do not represent the totality of privacy protections. In contrast, Konomi and Roussos praise Transport for London for the balance they have achieved between "loss of privacy and perceived benefit".[83] According to these authors, the facets of this balance include the following:

- Customers can tailor their privacy/benefit balance by using different types of cards. Anonymous cards bought for cash do not rely on personal information; however, this does not allow for the refund of credit on lost or stolen cards.
- The parties involved in the transaction of data and the use of that data are always clear in the Oyster card system as only TfL-operated machines can read or write card data.
- TfL has committed to providing appropriate safeguards to comply with the UK Data Protection Act and to clarify the use of data collected.[84]

Here, the fact that TfL sought advice on the use of personal data in contactless travel cards demonstrates an ethical stance and a concerted effort to take customers' data protection seriously and to act in a responsible, ethical manner.

Travel card operators develop and implement their own data protection or privacy principles, or solicit certification in relation to industry standards. For example, Octopus Card Limited who runs the Octopus Card in Hong Kong states the following:

---

[77] OECD, *Radio Frequency Identification (RFID)*, 2008, p. 6.
[78] European Commission, Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, (2009/387/EC), Official Journal of the European Union, L 122, 16 May 2009, pp. 47-51.
[79] Suzukit, Masataka, Kazukuni Kobara and Hideki Imai, "Privacy Enhanced and Light Weight RFID System without Tag Synchronization and Exhaustive Search", 2006 IEEE International Conference on Systems, Man, and Cybernetics, 8-11 Oct 2006, Taipei, Taiwan, and Langheinrich, 2009.
[80] Langheinrich, 2009.
[81] OECD, *Radio Frequency Identification (RFID)*, 2008, p. 6.
[82] OECD, "RFID Guidance and Reports", 2008, p. 63.
[83] Konomi and Roussos, 2007, p. 507.
[84] Ibid.

> As a responsible organisation, Octopus Cards Limited (OCL) values the importance of customer data privacy and protection, and is in full compliance with the related ordinances in handling customer data.
>
> Internal users are authorised to access the personal data on a need-to-know basis (eg hotline staff) and authentication is required before they are granted access to the data.
>
> We issue internal guidelines and conduct training for staff on the proper way to handle Octopus holders' personal information. We also have audit trails to monitor the use of such data and have regular internal audits and reviews to ensure strict compliance.
>
> We also issue policies on Personal and Customer Data Protection and Code of Practice to all employees on commencement of employment regarding the handling of data confidentiality and appropriate conduct in carrying out business. Employees are required to acknowledge receipt of and comply with these policies.[85]

Iarnród Eireann (Irish Rail), in relation to its smart card, state in its privacy policy that travellers' account details will not be shared with other companies and that individuals can remove the association between their account and the smart card, but they will only be able to top up the cards at vending machines and they will no longer be able to view their history on-line.[86] With regard to the processing of personal payments, a number of travel card providers have sought industry certification in order to ensure the secure collection of payment and to protect customer data. For example, Cubic Transportation Systems, which runs smart card schemes in 80 countries, has acquired Payment Application Best Practices (PABP) certification[87]. The PABP certification means that Cubic complies with the Payment Card Industry Data Security Standards, specifically they agree to the following: building and maintaining a secure network; protecting card holder data; maintaining a vulnerability management programme, implementing strong access control measures, regularly monitoring and testing networks and maintaining and information security policy.[88] Other payment security standards include the ITSO payment standard in the UK, VDV Standard in Germany, RKF in Sweden and EMV standards for open payment systems by contactless bank cards. Finally, the European Commission recognises the role that industry standardisation or certification can play in maintaining information security and privacy. They recommend that International Organization for Standardization (ISO) codes of conduct and best practices can help businesses manage information security and privacy, and that these codes and practices are compliant with EU regulations.[89]

Often the data generated by RFID chips on contactless travel cards and stored in databases associated with travel card systems are subject to data protection acts in different Member States and non-EU countries. According to van't Hof and Cornelissen, "the OECD Privacy Guidelines... square brackets with ellipsis are, in my view, redundant form the basis for many national laws on privacy… [and] state for example that people are entitled to know what kind of information is gathered about them, for a purpose specified in advance."[90] Transport for

[85] Octopus Holdings Limited, "Customer Data Protection", 2009.
[86] Iarnród Éireann, "Registration/Privacy", 2010. https://www.irishrail.ie/smartcard/pages/helpRegistrationIV.jsf
[87] Cubic Transport Systems, "A Credit to Cubic: New Software module ensures certified security for credit card data", *Collection Point: Quarterly Magazine*, No. 5, Dec 2008, p 24.
[88] PCI Security Standards Council, *Getting Started with PCI Data Security Standard*, October 2010, p.1. https://www.pcisecuritystandards.org/documents/PCI%20SSC%20-%20Getting%20Started%20with%20PCI%20DSS.pdf
[89] European Commission, 2009, p. 49.
[90] van't Hof and Cornelissen, 2006, p. 6.

London who run the Oyster Card system states that it complies fully with the UK Data Protection Act, and that individual travel records are kept for a maximum of eight weeks in order to assist with refunds or other enquiries.[91] They do not share the data with any third parties for commercial purposes; however, they do disclose information to law enforcement agencies on a case-by-case basis.[92] The original OV-chipkaart fell afoul of the Dutch Data Protection Act, when the Dutch Railways sought to offer personalised cards at cheaper rates than anonymous cards, in order to make use of customer data. The Dutch Privacy Chamber felt that the data retention approaches and the assumption that customers accepted the terms and conditions through use of the card were insufficient.[93] The Dutch Parliament intervened to ensure that both personalised and anonymous cards had to be offered at the same price, although anonymous cards could not be refunded when lost or damaged.[94] Outside the EU, the Identity Information Protection Act creates standards for all government-issued identification documents that contain RFID tags and helps California residents maintain a level of control, privacy, safety and security. Cards must be tamper-resistant, undergo an authentication process to prevent cloning and provide information about the technology and the privacy and security implications of the RFID-enabled card. When used in public transport, or if the card confers some other type of public benefit, the previous three conditions must be met, as well as one of the following:

> (1) a secondary verification and identification procedure that does not use radio waves; (2) a security protection, such as mutual authentication; (3) a security protection, such as encryption; and (4) a security protection, such as an access control protocol that enables the holder to exercise direct control over any transmission of the data using radio waves.[95]

In Japan, companies dealing with RFID tags and personal information must indicate that a tag exists on an item, give customers a choice regarding the use of tags, give information on the social benefits of tags and customer awareness, give information on the "linking of information on tags and databases that store privacy information", restrict information gathering and uses and ensure the accuracy of information stored on the tags.[96]

The use of RFID technologies in Europe is covered by the Data Protection Directive 95/46/EC and the Directive 2002/58/EC on privacy and electronic communications.[97] In these directives, Member States must ensure that the RFID applications used within their borders comply with data protection legislation, and state that industry should draw up Codes of Practice which can be reviewed at the national and EU level.[98]

Directive 95/46/EC states that:

- Personal data must be processed fairly and lawfully, and the purpose for which the data is collected must be explicitly specified. Information must also be accurate and up to date.
- Personal data may only be processed if the subject has given his/her explicit consent.
- The following personal data cannot be processed: "ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life", unless it is for a medical reason or some other vital purpose.

[91] van't Hof and Cornelissen, 2006, p. 10 and "Oyster data use rises in crime clampdown", 2006.
[92] Ibid.
[93] van Lieshout, et al., 2007, p. 213.
[94] van Lieshout, et al., 2007, p. 211.
[95] Ozer, 2008, para 61.
[96] Srivastava, 2007, p. 10.
[97] European Commission, 2009.
[98] Dehousse and Zgajewski, 2009.

- The data controller must provide the subject with information about the identity of the controller, the purposes of the processing, recipients of the data, etc.
- Subjects have a right of access to their data. They should be told whether data related to him/her has been processed as well as have a right to correct, erase or block the processing of their data.[99]

Although Directive 2002/58/EC outlines a number of guidelines for the providers of communications services, only the following are relevant for RFID-enabled travel cards:
Processing security, where they must ensure that personal data is accessed by authorised persons only, they must protect data from being destroyed, lost or altered accidentally and ensure that there is a security policy on the processing of personal data. If an infringement occurs, service providers must inform the person concerned and their national regulatory authority.
Confidentiality of communications, where communications made over a public electronic communications network must be confidential.
Data retention, where traffic and location data must be erased or anonymised when no longer required for billing purposes, unless consent has been given or in relation to national security or criminal investigations.
Controls, where Member States must implement a system of penalties, including legal sanctions, if the directive is infringed.[100]

Many of the different privacy-enhancing technologies, ethical principles, codes of practice, industry standards, Member State and other national legislation as well as European Directives, share some of the same principles and are thus overlapping. There is a clear orientation towards enabling anonymity, seeking informed consent, providing alternatives and rights of access. However, these different regulatory mechanisms also make the complexity of the privacy landscape in Europe in relation to RFID-enabled contactless travel cards apparent. The following discussion of future-oriented ethical rules or legal regulations attempts to streamline, simplify and provide over-arching principles to simplify this regulatory landscape.

2.6 NEED FOR NEW LEGISLATION, CODES OF CONDUCT, ETC. TO DEAL WITH PRIVACY IMPACTS NOT COVERED BY THE EXISTING FRAMEWORK AND HOW TO DEAL WITH ETHICAL ISSUES

While existing controls over privacy protection in relation to RFID-enabled travel cards, in the form of ethical rules, codes of practice, industry standards and EU and state legislation, offer individuals some protection over their personal data, it is largely accepted that these current rules and regulations are inadequate, especially given the pace of technological change and expansion of the uses of RFID.

Various researchers have offered their opinions on possible pathways for new rules and regulations to ensure the right to privacy, and the Article 29 WP has also been examining changes in the rules on RFID systems in depth. Van't Hof and Cornelissen have posited that a useful way of considering privacy in relation to the storage and use of personal data could be to consider "identity management". The notion of identity management would help theorists to

[99] Europa, "Protection of Personal Data", Summaries of EU Legislation, 1 Feb 2011. http://europa.eu/legislation_summaries/information_society/l14012_en.htm
[100] Europa, "Data protection in the electronic communications sector, 19 May 2010. http://europa.eu/legislation_summaries/information_society/l24120_en.htm

examine the interrelationships between "the owner/maintainer of the RFID environment and the user of this environment" and how "a person, interacting with an information system, defines what is known and not known about him/her to others using the system and how this relates to the information known or not known to the persons maintaining the system."[101] This would enable a mutual definition of identity. Taking a more specific approach, the OECD recommends that RFID systems should be transparent about the purpose of processing personal data and gain the consent of individuals who are affected.[102]

Systems should also include privacy notices that specify the existence of RFID tags, their content, use and control, the presence of readers in the environment, what they are reading, how tags can be disabled and where to find assistance.[103] Garfinkel et al. discuss an "RFID Bill of Rights" that includes many of the OECD guidelines as well as the right to "first-class RFID alternatives".[104] For example, customers should not lose the right to use particular roads, products or transportation options if they decline to participate in the RFID programme.[105]

In various Commission and Article 29 WP communications, forward-looking ethical principles and regulations have been recommended for the use of RFID, which are relevant for RFID-enabled travel cards. For example, the European Commission recommendation of 12 May 2009 states that RFID operators should minimise the processing of personal data and use anonymous or pseudonymous data wherever possible, and that operators should assess the privacy and data protection impacts of RFID applications prior to their implementation.[106] Operators should take appropriate measures to protect privacy, and these measures should be communicated to the relevant authorities as well as monitored and reviewed during the lifetime of the RFID application.[107] As part of this review of privacy impacts, operators should designate a person or group of people in the organisation who have responsibility for reviewing the assessments of privacy impacts, and to evaluate whether the measures in place remain appropriate for the protection of individual privacy. Finally, "Member States should ensure that operators develop and publish a concise, accurate and easy to understand information policy for each of their applications", that includes:

- the identity and address of the operators;
- the purpose of the application;
- what data are to be processed by the application, in particular if personal data will be processed, and whether the location of tags will be monitored;
- a summary of the privacy and data protection impact assessment;
- the likely privacy risks, if any, relating to the use of tags in the application and the measures that individuals can take to mitigate these risks.[108]

The Article 29 WP seeks to involve industry and other stakeholders as closely as possible in the decision-making process about how to balance the benefits of RFID technology applications. It undertook a large-scale consultation exercise in 2005, and invited industry to propose measures to address the privacy issues raised by RFID technologies. In 2011, the Article 29 WP issued recommendations based on a revised proposal submitted by industry for a privacy

[101] van't Hof and Cornelissen, 2006, p. 6.
[102] OECD, *Radio Frequency Identification (RFID)*, 2008.
[103] Ibid.
[104] Garfinkel, et al., 2005, p. 40.
[105] Ibid.
[106] European Commission, 2009, p. 48.
[107] Ibid.
[108] European Commission, 2009, p. 50.

and data protection impact assessment framework for RFID applications and that operators carry out privacy impact assessments (PIAs) for RFID applications. The working party recommended that a risk assessment phase begin the process, whereby the operators would characterise the application; identify risks to personal data by evaluating threats, their likelihood and their potential impact as well as compliance with European legislation; identify and recommend controls in response to risks identified; and finally, document the results of the PIA.[109] The revised framework also requires operators to consider how third parties may use the tags, particularly the risks that might arise if tags are carried by persons, as RFID-enabled travel cards are.[110] There are a number of layers to the revised framework. Specifically, not all applications of RFID will require the same level of assessment. If individuals simply carry RFID tags, they will only require a "'Small Scale PIA' (level 1)", while applications which also process personal data will require a "'full scale PIA' (level 2 and 3)", and applications where tags are not carried by individuals will not be subject to a PIA.[111]

2.7 CONCLUSION

The clear benefits of introducing RFID-enabled, contactless travel cards have driven the expansion of the market, from a few cities in the late 1990s to many dozens in 2011. Customers, industry, transportation companies, local authorities and police and security services all benefit from increased efficiency, and less congestion on public transport as well as the information collection capabilities that enable refunding, online or mobile top-ups to credit and theft protection. However, these benefits come with certain, specific risks to privacy, both through the exploitation of insecurities on cards, chips and back-end systems and the misuse of personal information. While a number of actors, including operators themselves, have sought to institute comprehensive protections, the following warning by Nicole Ozer remains appropriate:

> The best decisions about privacy and security are also less likely to be made when individuals are influenced by money and personal relationships. RFID in identification documents is big money and is expected to grow even larger.... [T]he global market for RFID was $1.94 billion in 2005 and...will likely reach $24.5 billion by 2015.[112]

Therefore, both current and future oriented ethical rules and legal regulations are necessary to protect individual privacy in such an expanding market. The Article 29 Data Protection Working Party has been working to consolidate various recommendations on the protection of RFID applications in general, and many of its recommendations are valid for RFID-enabled travel cards. However, its outputs, in the form of recommendations, are not legally binding. The European Commission and Member States must work proactively to ensure that transport passengers' personal information is protected from unwanted compromise, both through introducing privacy-enhancing technologies into the systems themselves, through introducing processes such as privacy impact assessments and through introducing laws and regulations which make these measures legally binding.

---

[109] Article 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, Adopted on 11 Feb 2011, p. 5. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

[110] Ibid., p. 6.

[111] Ibid., p. 4.

[112] Ozer, 2008, paragraph 53.

2.8 REFERENCES

Alfonsi, Benjamin J., "Privacy debate centers on Radio Frequency Identification", *IEEE Security and Privacy Magazine*, Vol. 2, No. 2, March-April 2004.

Article 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, Adopted on 11 Feb 2011. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

ASK, "Contactless Technology", 2011. http://www.ask-rfid.com/Technology/Contactless/tabid/101/language/en-US/Default.aspx

Bloomfield, Steve, "How an Oyster Card can Ruin your Marriage", *The Independent on Sunday*, 19 Feb 2006. http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html

Cavoukian, Ann, *Privacy by Design: Take the Challenge*, Information and Privacy Commissioner of Ontario Canada, Toronto, March 2009.

Calypso Networks Association, "Implementations", 2011. http://www.calypsonet-asso.org/index.php?rubrique=main_50

Cubic Transportation Systems, "Enterprise systems for transit", 2011. http://cts.cubic.com/Solutions/EnterpriseSystemsforTransit/tabid/363/language/en-US/Default.aspx

Cubic Transportation Systems, "Case Study: London Oyster® Card System", 2011. http://cts.cubic.com/Customers/UnitedKingdom/CaseStudyLondon/tabid/430/language/en-GB/Default.aspx

Cubic Transportation Systems, "Cubic Signs $220 Million Contract to Design, Build, Operate and Maintain Vancouver Smart Card and Faregate System", press release, 27 Jan 2011.http://cts.cubic.com/AboutUs/News/News/tabid/434/articleType/ArticleView/articleId/30/language/en-GB/Cubic-Signs-220-Million-Contract-to-Design-Build-Operate-and-Maintain-Vancouver-Smart-Card-and-Faregate-System.aspx

Cubic Transportation Systems, "Mobile and Contactless Payment", 2011. http://cts.cubic.com/Solutions/MobileandContactlessPayment/tabid/365/language/en-GB/Default.aspx

Cubic Transportation Systems, "Case Study: Los Angeles TAP® Card System", 2010. http://cts.cubic.com/Customers/UnitedStates/CaseStudyLosAngeles/tabid/427/language/en-US/Default.aspx

Cubic Transport Systems, "A Credit to Cubic: New Software module ensures certified security for credit card data", *Collection Point: Quarterly Magazine*, No. 5, Dec 2008.

Cubic Transport Systems, "Getting Smart in San Francisco", *Collection Point: Quarterly Magazine*, No. 3, June 2008.

Cubic Transport Systems, "Beyond the Gate: An engineer's-eye-view on emerging ticketing and gating solutions across Europe", *Collection Point: A bi-monthly magazine for Europe*, No. 2, March 2008.

Cubic Transport Systems, "The World is their Oyster", *Collection Point: A bi-monthly magazine for Europe*, No. 1, Dec 2007.

Dehousse, Franklin, and Tania Zgajewski, "RFID: New 'Killer Application' in the ICT World, New Big Brother or Both?", *Egmont Paper 30*, Academia Press, Gent, June 2009.

Europa, "Protection of Personal Data", Summaries of EU Legislation, 1 Feb 2011. http://europa.eu/legislation_summaries/information_society/l14012_en.htm

Europa, "Data protection in the electronic communications sector", 19 May 2010. http://europa.eu/legislation_summaries/information_society/l24120_en.htm

European Commission, Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, (2009/387/EC), Official Journal of the European Union, L 122, 16 May 2009, pp. 47-51.

Garfinkel, Simson L., Ari Juels and Ravi Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", *IEEE Security & Privacy Magazine*, Vol. 3, No. 3. 2005, pp. 34-43.

The Guardian, "Oyster data use rises in crime clampdown", 13 March 2006. http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation

GVB, "What is the OV-chipkaart", 2011. http://www.gvb.nl/english/travellers/tickets-and-fares/ov-chipkaart-travel-products/pages/what-is-the-ov-chipkaart.aspx

Iarnród Éireann, "Registration/Privacy", 2010. https://www.irishrail.ie/smartcard/pages/helpRegistrationIV.jsf

Konomi, Shin'ichi and George Roussos, "Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments", *Perspectives on Ubiquitous Computing*, Vol. 11, 2007.

Korea Smart Card Co., "T-Money Service", 2006. http://eng.t-money.co.kr/

Korea Smart Card Co., "Korea Smart Card Co., Ltd.", 2006. http://eng.t-money.co.kr/

Langheinrich, Marc, "A survey of RFID privacy approaches", *Personal and Ubiquitous Computing*, Vol. 13, No. 6, 2009.

Miller, Vikki, "Oyster card: fears over Mifare security", *The Telegraph*, 21 June 2008. http://www.telegraph.co.uk/news/newstopics/politics/2168791/Oyster-card-fears-over-Mifare-security.html

Octopus Holdings Limited, "Corporate Profile: Hong Kong Services", 2009. http://www.octopus.com.hk/about-us/corporate-profile/services-in-hong-kong/en/index.html

Octopus Holdings Limited, "Customer Data Protection", 2009. http://www.octopus.com.hk/customer-service/faq/en/index.html#Service05

Organisation for Economic Cooperation and Development (OECD), "RFID Guidance and Reports", *OECD Digital Economy Papers*, No. 152, OECD publishing, 2008.

OECD*, Radio Frequency Identification (RFID): A Focus on Information Security and Privacy*, DSTI/ICCP/REG(2007)9/FINAL, OECD Publishing, 14 Jan 2008.

Ozer, Nicole A., "Rights 'Chipped' Away: RFID and Identification Documents", *Stanford Technology Law Review*, Vol. 1, Jan 2008. http://stlr.stanford.edu/pdf/ozer-rights-chipped-away.pdf. See also Dehousse and Zgajewski, 2009.

PCI Security Standards Council, *Getting Started with PCI Data Security Standard*, October 2010. https://www.pcisecuritystandards.org/documents/PCI%20SSC%20-%20Getting%20Started%20with%20PCI%20DSS.pdf

Railway Procurement Agency, "ITS FAQs", 2008. http://www.rpa.ie/en/its/Pages/ITSFAqs.aspx#anchor_use

Ramos, Alan, Weina Scott, William Scott, Doug Lloyd, Katherine O'Leary and Jim Waldo, "A Threat Analysis of RFID Passports: Do RFID passports make us vulnerable to identity theft?", *Communications of the ACM*, Vol. 52, No. 12, Dec 2009, pp. 38-42.

Rieback, Melanie R., Bruno Crispo and Andrew S. Tanenbaum, "Is your cat infected with a computer virus?", *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, 2006, pp. 169–179.

Rotter, Paweł, "A Framework for Assessing RFID System Security and Privacy Risks", *Pervasive Computing*, April-June 2008, pp.70-77.

Srivastava, Lara, "Radio frequency identification: ubiquity for humanity", *info*, Vol. 9, No. 1, 2007, pp. 4-14.

Suzukit, Masataka, Kazukuni Kobara and Hideki Imai, "Privacy Enhanced and Light Weight RFID System without Tag Synchronization and Exhaustive Search", 2006 IEEE International Conference on Systems, Man, and Cybernetics, Taipei, Taiwan, 8-11 Oct 2006.

Thompson, Iain, "Oyster card system clams up; Glitch wipes 40,000 cards", *vnunet.com*, 15 Jul 2008. http://www.v3.co.uk/vnunet/news/2221591/oyster-card-system-clams

Thompson, Rebecca, "Cubic takes on Transport for London's Oyster card IT contract", *ComputerWeekly.com*, 17 Aug 2010. http://www.computerweekly.com/Articles/2010/08/17/242418/Cubic-takes-on-Transport-for-London39s-Oyster-card-IT.htm

van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij, Claudio Borean, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, Office for Official Publications of the European Communities, Luxembourg, 2007.

van't Hof, Christian, and Jessica Cornelissen, *RFID and Identity Management in Everyday Life: Case Studies on the Frontline of Developments towards Ambient Intelligence*, European Technology Assessment Group, Oct 2006.

Chapter 3, Privacy, data protection and policy issues in RFID enabled e-Passports

Raphaël Gellert and Serge Gutwirth
Vrije Universiteit Brussel

3.1 INTRODUCTION

This case study focuses on the e-passport from the point of view of RFID technology.
The perspective chosen is the following one: the "hard", normative choices and discussions are left for chapter 6. This document acknowledges the reality of the biometric passport and therefore focuses on how to implement this technology in the best possible manner as far as fundamental rights are concerned, in particular with respect to data protection principles (and consequently privacy as well).

After a general introduction on RFID, it introduces and contextualises the introduction of RFID-enabled passports in response to events in late 2001. The chapter continues by identifying the stakeholders involved in the introduction of RFID enabled passports and their relative positions, including government stakeholders, international organisations, industry players, non-government organisations and end users. The next section outlines some potential privacy infringing issues in relation to RFID enabled passports. These include issues surrounding the security of the chips and back end systems, data processing operations which threaten privacy, such as unauthorised reading or clandestine tracking, and the specific privacy violations which could arise from these data processing operations. This is followed by a discussion of the ways in which both the e-Privacy Directive and the Data Protection Directive may mitigate these privacy concerns. The chapter concludes with a number of recommendations surrounding future-oriented regulatory instruments that could address some of the privacy infringements not currently considered under existing legislation, for example, issues such as consent, the right to be informed of how data is being processed and rights of access. The chapter argues that technical solutions such as privacy by design or privacy impact assessments could address some of the potentials for privacy infringement. However, there is a clear need for technology-specific, tailor made legislation.

3.2 RFID – STATE OF THE ART

RFIDs can be classified as automatic identification (auto-id) systems. The function of such systems is to provide automatic identification of objects. In this sense, they have been described as the new generation of barcodes.[113] However, RFIDs have broader functionalities, like data storage, or computational capabilities (which brings them closer to smartcards).[114] Because of these capacities, RFIDs are considered as the necessary backbone to the "Internet of things" scenario.

An RFID system is composed of three elements: a RFID tag, a reader, and the backend system (i.e., middleware and applications).[115]

3.2.1 RFID tags

RFIDs tags are electronic chips (they can be as small as 0.3 mm^2)[116] implemented within just any kind of products and objects. Joint with a thin film antenna, they form a tag that is at-

[113] Spiekermann, Sarah, *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*, Shaker Verlag, Aachen, 2008, p. 56.
[114] Henrici, Dirk, *RFID Security and Privacy – Concepts, Protocols, and Architectures*, Springer, Berlin, 2008, p. 7.
[115] Henrici, 2008, p. 8.
[116] Speikermann, 2008, p. 55.

tached to the object within which they are implemented, and which serves to identify the latter by associating it to its tag number. These tags can be read by RFID readers, which read the information that is contained in the chip from a distance that varies according to the radio frequency spectrum used (cf. *Infra*, RFID reader).[117]
Therefore, RFID tags are constituted by three elements: a chip, an antenna, and the packaging/encapsulation of the two former.[118]

Nowadays, RFID tags are composed of semiconductor materials like silicon compounds or copper, whilst antennas are built from aluminium. Future prospective includes tags being built out of polymeric or organic materials.[119]

RFIDs can take many forms, but the main taxonomy that can be operated is between active and passive RFID tags. Active RFID tags can self-initiate the sending of the data they contain (this is made possible because of their own energy source). Passive RFID tags on the contrary need to be activated by a reader in order to send their data.[120] In other words, passive tags have no power-supply and communicate with the reader using the energy of the latter, whereas active tags have their own power source.
There also exists hybrid forms known as semi-active tags, which although having their own power supply, still use the energy of the reader when communicating with the latter.[121]
Passive and active tags both have their advantages and disadvantages. The advantages of passive tags include their low price (they are thus more widely spread), their small size, low weight, and a longer lifetime, since it is not restricted by battery life. On the other hand, active tags have a wider reading range, and can be used for various applications.[122]

The functionalities of RFID tags will therefore depend upon the passive or active nature of the chip.
Therefore, besides their traditional function of storing data to be read by readers, RFID tags can also have computational capabilities, e.g., password check or ciphering algorithms, or tags with sensors for telemetry-related applications.[123]

3.2.2 RFID readers

RFID readers read the information that is sent by the tag through its antenna (although they can also send some information to the tags). Furthermore, they are connected to the back-end system to which they send the information retrieved from the tag. They are composed of an antenna, a chip, and an interface (which is used to communicate with the back end system). As mentioned earlier, the power supply of the reader is also used to activate passive tags. There are two types of readers, stationary readers that are fixed, and mobile readers.[124]

RFID tags communicate the information they contain to readers through electromagnetic means. This entails that no wiring between the two is required, nor a line of sight.[125]

---

[117] Ibid.
[118] Henrici, 2008, p. 9.
[119] Ibid, p. 10.
[120] Speikermann, 2008, p. 56.
[121] Henrici, 2008, p. 10.
[122] Ibid.
[123] Ibid, pp. 10-11.
[124] Ibid, p. 12.
[125] Ibid, p. 13.

Different frequencies are used, depending upon the characteristics of the tags (i.e., active/passive), the environment, their use, etc.[126]

3.2.3 RFID backend systems and middleware

RFID systems are not only composed of tags and readers. Indeed, readers will query tags for reading/writing data. However, the data that is read needs to be further processed, whereas the written data needs to be available. Therefore, an additional element is required: the backend system.

Backend systems can be divided into two parts: the actual applications software, and the middleware, which acts as a buffer between the tag-reader unit, and the application software of the backend system.
Middleware are used to aggregate and filter data, and to provide an open and neutral interface towards the applications. It can decouple applications and specific tag and reader characteristics (i.e., special protocol, proprietary standards…).
Finally the software application will process the data accordingly.[127]

Although tags and backend systems have different purposes within a RFID system, their role may overlap as far as the storing of data is concerned. Indeed, there are two possibilities where tag information can be stored. Either, it can be directly stored on the tag, either, it can be stored within a backend database. If data is stored in the database, the corresponding tag needs only to carry a sole information: a unique identifier that is used as a key to the database, and which thus ultimately links the tag to the relevant data.[128] Both approaches have their advantages and disadvantages.

3.2.4 RFID functionalities

As an auto-id system, a RFID system is a data processing device. The whole point of the system is to transmit information from the tag to the reader, and from the reader to the backend system. RFID tags can carry any sort of information. For instance, they can carry the date of manufacturing, minimum durability, batch number, etc.
It can therefore be argued that its core functionality is to identify tags. The identification of the tag will take place through a query of the reader. However, thanks to its capabilities, RFID system can be more than an "upgraded barcode". Indeed, additional information can be associated to a tag, as is the case in logistics, with supply-chain of applications that inform about products' expiry date, tracking assets, reducing out of stock, etc. One application of particular interest, which uses associated data, is to give assistance to people. One example is the so-called "intelligent home" that features smart appliances like a microwave oven that automatically detects how to best cook a certain type of food. Going a step further, exists the possibility of equipping tags with additional information and computational capabilities. This is the case of tags equipped with sensors, which can be used for telemetry (e.g., monitoring cooling chains), or tags with geolocation capabilities.[129] Because of these functionalities, RFID goes beyond than the mere identification of objects, and this entails that tags not only contain information relating to an object, but also, eventually personal information of individuals.

---

[126] Ibid, p. 14.
[127] Ivantysynova, Lenka, Ziekow, Holger, "RFID in Manufacturing: From Shop Floor to Top Floor, in Günther, Oliver, Wolfhard Kletti and Uwe Kubach (eds.), *RFID in Manufacturing*, Springer, Berlin, 2008, p. 7.
[128] Henrici, 2008, p. 20.
[129] Ibid, 2008, p. 21.

It is in this respect that RFIDs are seen as the backbone of the so-called Internet of things scenario, wherein the Internet not only connects computers and communication terminals, but also any existing objects.[130] Indeed, as an auto-id system, RFIDs are a means to the digitalisation o the phenomenal world. As such, they can deliver a whole new range of services and applications.[131]

Because RFIDs can indeed be used for a whole range of applications, a RFID reference model has been created, which taxonomizes the different field of applications where RFID can be used. The main distinction it makes is between application where the tag contains personal data of individuals, and applications where the tag only contains object information.[132]

Reference	RFID Application fields	Description
Mainly Object Tagging	A. Logistical tracking & tracing	Identification and location of goods (e.g. pallets or containers)
	B. Product safety, quality and information	Applications to ensure quality (e.g. sensors to monitor temperature) and product safety (e.g. fight against counterfeiting)
Tagging with reference or potential reference to people	C. Access control and tracking & tracing of individuals	Single function tags for identification and authorisation applications for entries and ticketing
	D. eHealth care	Systems for hospital administration and smart systems to support and monitor health status
	E. Public services	Systems mandated by law or to fulfill public duties (e.g. ID-cards, health insurance cards, road tolling systems)

3.2.5 The e-passport

The e-passport, or Machine Readable Travel Document (MRTD) can be understood as an application of Identity Management Systems (IMS). IMS can be defined as technical systems supporting the process of management of identities.[133] In this respect and in Europe, e-passports contain biometric data of individuals that is stored on a RFID chip in the passport.[134] The e-passports itself thus consists of a contactless microprocessor chip (the RFID tag) that is laminated into the passport data page or integrated into the passport cover.[135] The main application of RFID in IMS remains for the e-passport, which is for us, maybe the most

[130] European Commission, Radio Frequency Identification (RFID) in Europe: Steps towards a policy framework, COM(2007)96 final, 15 Mar 2007, p. 3.
[131] Ibid.
[132] Ivantysynova, et al., 2008, p. 10.
[133] Meints, Martin, and Mark Gasson, "High-tech ID and Emerging Technologies", in Rannenberg, Kai, Denis Royer and André Deuker (eds.), *The Future of Identity Systems in the Information Society – Challenges and Opportunities*, Springer, London, 2009, p. 131.
[134] van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij and Claudio Borean, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, Office for Official Publications of the European Communities, Luxembourg, 2007, p. 191.
[135] Finkenzeller, Klaus, *The RFID Handbook – Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, third edition, Wiley, Chichester, 2010, p. 380.

interesting. But RFID is also used in other ID-cards, such as financial cards, university cards, driving licences, etc.[136] Biometrics in turn can be defined as the automated recognition of individuals, based upon biological and/or behavioural characteristics.[137]

Several reasons have been put forward to justify the use of RFID in biometric passports. They include the fact that it can provide better document security (passport become harder to counterfeit, it can facilitate the inclusion of biometric data because of the potentially higher memory capacity of RFID tags, and many members of the UN International Civil Aviation Organization (ICAO) are adopting it.[138] RFID is also more promising because maintenance cost are lower since the cards are not subject to wear and tear caused by friction when a contact card is inserted into a reader (as opposed to a contactless, RFID card that is read from distance). Also, according to article 1(2) of the EU Regulation (EC) 2252/2004 on standards for security features and biometrics in passports and travel documents issues by Member States, "the data shall be secured, and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data". In its Decision of February 2005, the European Commission opted for the RFID, which, according to the institution fulfilled the criteria of the Regulation.[139] Maintenance costs are also lower since the components can be shielded in a protective case. This in turn, allows for operations in harsh environments, and longer lifespan.[140] In addition to that, RFID allows for higher data rates, and does not require a change of the format of the passport (e.g., credit card format).[141] Also, RFID technology is much easier to use in the context of passport verification.[142] In sum, RFID seems to be a technology that meets the demands with respect to usability, data capacity, and performance.[143] However, our following analysis of privacy and security issues of RFID in the e-passport will mitigate this statement.

E-passport in Europe: present situation

As a result of the US adoption of the biometric passport and its ensuing endorsement by the ICAO, the EU also resorted to this technology.[144]

Different types of EU legislations apply to the e-passport.

First, there exists specific legislation regulating the passport as such. It is composed of the EU Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security fea-

[136] van Lieshout, et al., 2007, pp. 189-190.
[137] Meints and Gasson, 2009, p. 138.
[138] van Lieshout, et al., 2007, p. 194.
[139] European Commission, Decision K (2005) 409 of 28 February 2005, of which the French text is available at http://europa.eu.int/comm/justice_home/doc_centre/freetravel/documents/doc/c_2005_409_fr.pdf. No official English is text available because the United Kingdom and Ireland have not taken part in the adoption of this measure.
[140] van Lieshout, et al., 2007, p. 191.
[141] Hoepman, Jaap-Henk, Engelbert Hubbers, Bart Jacobs et al., "Crossing Borders: Security and Privacy Issues of the European e-Passport", in Yoshiura, Hiroshi, Kouichi Sakurai et al. (eds.), *Advances in Information and Computer Security. Proceedings of the First International Workshop on Security*, IWSEC 2006 Kyoto, 23-24 Oct 2006, Springer, Berlin, 2006, p. 153.
[142] *Avoine, Gildas,* Kassem Kalach, Jean-Jacques Quisquater, *"E-passport: Securing International Contacts with Contactless chips", Lecture Notes in Computer Science, Vol 5143/2008, 2008, p. 142.*
[143] International Civil Aviation Organisation (ICAO), *Technical Report – Biometrics Deployment of Machine Readable Travel Documents*, Version 2.0, 2004, p. 35.
[144] All countries part of the Visa-Waiver Program were mandated by the US to adopt the passport. See, Pooters, I., *Keep out of My Passport: Access Control Mechanisms in E-passports*, 2008, p. 1. http://www.avoine.net/rfid/

tures and biometrics in passports and travel documents issues by Member States.[145] This Regulation established the characteristics of the new EU passport, and the modalities of the adoption of the document by the Member States, and was to be fully implemented by August 2006. According to the Regulation, the biometric features must comply with the standards developed by the ICAO in its Document 9303.
It was further refined by two Decisions from the European Commission, namely, the Commission Decision (C(2005)409 of 2005,[146] and Commission Decision (C(2006) 2909 of 2006.[147] The first Decision established the technical standards regarding security features and the use of biometrics of the e-passport. At the time of this decision, the only biometrics used was the facial image. It also provided for a deadline regarding the implementation of the document, i.e., 28 August 2006. The second Decision contains additional security standards and foresees that fingerprints shall be used as an additional biometric identifier in the European e-passport. Its provisions officially entered into force in June 2009.[148]

In other words, EU legislation is limited to the harmonisation of security and biometric features. Other issues such as the storage of the biometric data (on-tag or in a backed system) remains within the competences of the Members States. Article 4 however, concerns the protection of privacy and personal data of citizens, as it foresees that passport holders have the right to verify the data inserted in their passport, and where appropriate, to rectify/erase such data.[149]

As far as today, e-passports are being used in all 27 EU member States. Some States have already started issuing second-generation passports (with fingerprints). This is the case for Austria, Estonia, Finland, France (2009), Germany (2007), Greece, Hungary (2009), Italy (2010), Luxembourg, The Netherlands, Poland (2009), Romania (2010), Slovenia, Spain, and Sweden (2009). It is estimated that in 2009 e-passports accounted for 57% of all passports issued, and 28% of all passports circulating. This should normally culminate in 2014, where e-passports will represent 88% of all passports issued (and 80% of all passports circulating).[150] [151]

[145] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *Official Journal, L 385, Vol. 37, 29 Dec 2004, pp. 0001 – 0006.*
[146] Commission Decision (C(2005)409 of 28 February 2005 establishing the technical specification on the standards for security features and biometrics in passports and travel documents issued by Member States.
[147] Commission Decision (C(2006) 2909 of 28 June 2006 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.
[148] European Commission Joint Research Centre, Security Technology Assessment Unit. http://sta.jrc.ec.europa.eu/index.php/technical-challenges-for-identification-in-mobile-environments
[149] Article 4(1) states that: "Without prejudice to data protection rules, persons to whom a passport or travel document is issued shall have the right to verify the personal data contained in the passport or travel document and, where appropriate, to ask for rectification or erasure."
[150] Acuity Market Intelligence, *ePassport Market Adoption to Reach 88% by 2014*, 2011, p. 1. http://acuity-mi.com/PR%20GePPeV%202.pdf
[151] Finkenzeller, 2010, p. 381. See also, **European Commission Decision C(2006) 2909 final of 28 June 2006, annexe, pp. 4-5.** http://www.statewatch.org/news/2008/feb/eu-biometric-passports-dec-2006-fr.pdf

3.3 STAKEHOLDERS AND DRIVERS BEHIND THE DEVELOPMENT OF THE TECHNOLOGY

3.3.1 Governments

The biometric passport attained worldwide use after the US government started advocating for its use in the aftermath of the events of 11 September 2001. In the wake of these tragic events, and of the failed 22 December 2001 attack by Richard Reid (known as the "shoe bomber"), the US government decided to tackle what appeared to be a problem of effective immigration management and counter terrorist risk through the use of an information technology device: the electronic passport.[152]

The biometric passport thus responded to the need to enhance border control in several ways. As one commentator put it, the e-passport was seen as the answer to the question: How to mitigate terror threats, manage illegal entry while also attracting visitors?[153]
First, biometric technology was thought of as a means to have more secure identification.
Second, the technology used (both biometric and contactless RFID chips) was conceived as means to fight against identity theft, passport tampering and forgery.
Finally, the e-passport technology was also understood to be an effective means for identity control that wouldn't put at jeopardy the entire Visa Waiver Program, which would have resulted with sever economical losses for the US government.
Finally, the use of automated identity recognition technology also represents savings and economic benefits in terms of human investments at borders.[154]
All in all, the e-passport can be described as a technological device that offers the possibility of producing a machine-determinable match between person and document, thereby enabling for a retooling of the immigration control process, which entails, inter alia, the cutting of costs in this area.[155]

3.3.2 International Organisations

As far as the electronic passport is concerned, International Organisations have played a standard setting role, especially the ICAO in collaboration with the ISO.

Indeed, the US government, which is at the origin of the introduction of the e-passport, has called upon the expertise of the ICAO at several occasions.

First, the Patriot Act, although implicitly, mandated to work with the ICAO on meeting the "internationally accepted standards for machine readability".[156]
But whereas, the Patriot Act only contained a machine-readable clause, the later Enhanced Border Security and Visa Entry Reform Act (also known as the Border Security Act) of 2002 provided for the use of the biometric passport. As a matter of fact, the Act foresees that e-passports must be "tamper-resistant and incorporate biometric and document authentication

[152] Bronk, Christopher, *Innovation By Policy: A Study of the Electronic Passport*, 2007, pp. 4-7. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1557728
[153] Ibid. p. 9; van Lieshout et al., 2007, p. 197.
[154] Bronk, 2007.
[155] Bronk, 2007, p. 18.
[156] Ibid., p. 22.

identifiers that comply with applicable biometric and document identifying standards established by the International Civil Aviation Organization".[157]
In other words, the Border Security Act required the creation of a new technical standard, incorporating a mechanism for passing biometric information from the passport of a foreign country to a computerized machine. This required new technical standards that would be fixed by the ICAO, in collaboration with the ISO, and the US government. Indeed, the U.S. State Department has worked in close collaboration with the ICAO (and has relied upon the latter) in order to set both the standard for biometric component for electronic passports (i.e., MRTDs), and the standards of the microchip wherein these biometric components would be embedded.[158]
In its 2002 Berlin Resolution, the ICAO's New Technologies Working Group (NTWG) endorsed facial recognition as the biometric identifier (although it didn't preclude from the use of other biometric elements, such as fingerprints, cf. the EU e-passport). For the format of the facial image, the NTGW selected the ISO 10198 Standard, commonly referred to as the JPEG format. As far as the microchip is concerned, the ICAO has opted for RFID contactless technology, in conformity with the ISO 14443 standard.[159]

3.3.3 Industry Players

Corporate players are an important driver behind the biometric passport as it represents a substantial market.
For instance, in the United Kingdom, IBM and CSC were awarded the contracts to run some of the technology underpinning the government's biometric passport scheme. IBM was awarded a £265m contract to craft and run the national database containing fingerprints and facial images. Equally, CSC was awarded a £385m contract.[160]
The French Germalto Corporation is another important economic player in the e-passport market. Smartcard constitute its core business (it is said to be the market's world leader) and a third of its activities are devoted to security, and more specifically, to electronic passport and Identity Management.[161] It has implemented the electronic passport in many countries, among which, Denmark, the United States, France, Norway, Poland, Portugal, the Czech Republic, Russia, Singapore…[162]

3.3.4 Non-Governmental Organisations

Just as with any other public policy issue, Non Governmental Organisations (NGOs) are an important stakeholder. In the debate surrounding the biometric passport, they have voiced much criticism against the electronic passport. For instance, civil society organisations have criticised the electronic passport concerning its security and privacy features. The American Civil Liberties Union (ACLU) has underlined flaws in its protection from monitoring, replication and manipulation.[163] This advocacy work has been so successful that it has led the ICAO

[157] US Congress, Enhanced Border Security and Visa Entry Reform Act of 2002, Public Law 107-173, 107th Congress, 2nd Session, 14 May 2002.
[158] Bronk, 2007, pp. 23-24.
[159] Ibid., 2007, pp. 25 & 32.
[160] Espiner, Tom, "IBM, CSC win ID card biometrics contracts", ZDNet, 7 April 2009. http://news.zdnet.co.uk/security/0,1000000189,39637650,00.htm
[161] Le Point, "Gemalto", 25 September 2008. http://www.lepoint.fr/archives/article.php/277010
[162] PR Newswire Europe, "L'Etonie retient Gemalto pour sa solution de passeport électronique", 2011. http://www.prnewswire.co.uk/cgi/news/release?id=182028
[163] See, Schneier, Bruce, "The Id Chip You Don't Want to see in Your Passport", *The Washington Post*, 16 Sept 2006.

to change its position on the cryptography of passports. Whereas it first deemed cryptographic devices unnecessary, the security shortcomings outlined by Civil Society Organisations have convinced it to incorporate some basic security features, including electronic signature, cryptographic mechanisms such as the Basic Access Control (BAC), and a so-called Faraday Cage, that is, a metallic shielding imbedded in the passport cover and designed to protect if from electronic eavesdropping.[164]

3.3.5 End users

End users might benefit from the e-passport in several ways.

One of the most frequently cited benefits that users might get from the biometric passport is convenience. Indeed, users, and especially those benefiting from a Visa Waiver, will see their waiting time at border control shrink, thanks to the contactless RFID technology embarked in the passport. This was for example the case in Malaysia, where it was possible to clear a passenger in 15 seconds, without the need for human intervention.[165] The amount of saved time during border control becomes thus considerable.[166]
E-passports are also convenient as they are seen as a milestone device in enabling a whole range of e-services (amongst which e-government but not only) to be offered to citizens. Indeed, e-passports would bring more trust, easy access, or convenience. In this respect, they would certainly contribute to creating a better-integrated European information society.[167]

Furthermore, and as mentioned earlier, governments have resorted to e-passports as a tool to fight against passport forgery and the resulting identity theft. This is also of great advantage to users. Because modern, non-biometric passports are hard to forge, criminal organisations do not even try such fraud, but instead collect large numbers of genuine passports, and pick one that shows a reasonable resemblance to a member that needs a new identity. Similarly, passports are sometimes borrowed for illegal border crossing, and later returned to the rightful owner.
The original aim of the use of biometrics in travel documents is thus to combat "look-alike" fraud. Hence the emphasis is on biometric verification.[168] Hence, passport forgery becomes more difficult because of the technical characteristics of the passport, and because the bond between the passport and the document holder is strengthened.[169]

However, there are also some disadvantages attached to the use of the biometric passport. One of them is the price of the item. Indeed, the introduction of electronic passports represents additional costs for citizens. In the United Kingdom for example, it has represented an estimated cost for the government (and hence taxpayers) of more than £5.6 billion over next 10 years (period 2007-2017).[170] Equally, the price for buying the passport has substantially in-

[164] Bronk, 2007, pp. 30-31 and 35.
[165] Ibid., p. 20.
[166] Gipp, Béla, Jöran Beel, and Ivo Rössling, *ePassport: The World's New Electronic Passport*, 2007, p. 11. www.epassport-book.com
[167] van Lieshout et al., 2007, p. 197.
[168] Hoepman et al., 2006, p. 153.
[169] Gipp, et al., 2007, p. 11.
[170] BBC News, "ID card scheme 'to cost £5.6bn'", 8 Nov 2007. http://news.bbc.co.uk/2/hi/uk_news/politics/7084560.stm; The Guardian, "Cost of ID cards rockets by £840m", 10 May 2007. http://www.guardian.co.uk/politics/2007/may/10/idcards.immigrationpolicy

creased in comparison to its former (paper) version, reaching costs that have been described by many as being excessive.[171]
But the main disadvantage associated to the e-passport for end-users certainly lies in the many security flaws and consequent privacy infringements.

3.4 PRIVACY AND SECURITY ISSUES

In the framework of RFID, and more specifically of the biometric passport, there are several data processing operations that threaten the privacy of individuals in different ways, and relate to different kinds of privacy. As a matter of fact, some of these operations are made possible because of shortcomings in the security of e-passports, such as cryptographic and digital signature weaknesses, or the vulnerability of protection devices such as the Faraday Cage.
The chosen perspective is the following one: the security and privacy threats will be analysed in the light of the e-passport primarily understood as an RFID device.

3.4.1 Shortcomings in the security of the passport

As aforementioned, initially no security devices were foreseen re the biometric passport until Civil Society Organisations raised awareness among the ICAO concerning the threats to which the passport could be exposed (cf. *supra*, Non Governmental Organisations).[172] Consequently, the ICAO developed some protection mechanisms to be implemented in the document.[173]

E-passports now feature a digital signature. According to this mechanism, authorised entities that also produce the passport (e.g., printing companies) use a secret code for electronically signing the document. Equally, a public code is used to verify the authenticity of the electronic document. The country's certification authority issues this code.[174]

In addition to the electronic signature, the ICAO has introduced a series of optional cryptographic measures, the best-known being the Basic Access Code (BAC).[175]

Passive authentication allows the reader to verify the authenticity of the data stored in the RFID tag.[176] Active authentication prevents the copying of the microprocessor through the use of a Private Key: the passport proves that it possesses the Key, which is stored in a secure memory.[177] For the second generation of passport that contain additional biometric information (i.e., fingerprints), the ICAO has recommended the recourse to Extended Access Control (EAC), but has not standardized it yet. The European Union has pioneered this mechanism,

[171] Le Point, "Le prix des passeports pourrait augmenter", 3 Oct 2008. http://www.lepoint.fr/archives/article.php/279393; Le Point, "Le passeport biométrique, une manne pour l'État", 1 July 2010. http://www.lepoint.fr/societe/le-passeport-biometrique-une-manne-pour-l-etat-01-07-2010-1209696_23.php; The Guardian, "Cost of ID card and passports rises to £100", 9 Nov 2007. http://www.guardian.co.uk/uk/2007/nov/09/idcards.politics.
[172] Meingast et al., 2007, p. 44.
[173] Bronk, 2007, pp. 30-31.
[174] Finkenzeller, 2010, pp. 381-382.
[175] The BAC has however been implemented in most, if not all, e-passports.
[176] Pooters, 2008, p. 4.
[177] Pooters, 2008, p. 5.

and has released a first version in 2006.[178] The BAC is an encryption scheme designed to permit the transmission of data only to an authorised reading device. In order to communicate with the passport, the reader needs a key to access the information on the tag. Once it has established a communication with the RFID, the ensuing reading of information is encrypted. This requires that the passport must be intentionally shown and read before access to the tag is allowed.[179] BAC is meant to prevent passport reading without the holder's involvement, i.e., mainly skimming and eavesdropping.[180]

Unfortunately, gaps have been discovered in these protection mechanisms. IBM researchers have determined that the digital signature regime would make counterfeiting actually… easy. Indeed, it is possible for a forger to splice together a valid electronic signature with false identity information and biometric components.[181]

As far as the BAC is concerned, a Dutch computer security expert discovered that the passport encryption scheme of his country could be defeated in less than two hours by a personal computer generating all possible key sequences, and that the RFID chip could be cloned using the same process.[182]
Equally, German Security consultant Lukas Grunwald famously managed to clone a chip, but was not however able to clone the data stored on it in an undetectable manner.

In addition to that, another security mechanism was foreseen: a Faraday Cage, i.e., a metallic shield to the cover of the passport to prevent skimming and other unauthorized data processing operations.[183]
The idea behind the Faraday Cage is to prevent the unauthorised reading of e-passports through the use of a passport cover that is made of opaque, Radio Frequency blocking materials (e.g., aluminium fibre).
Hence, the only way to access the information protected by a Faraday Cage is to, literally, open the cage that is opening the passport. The catch faced by the Faraday cage lies in the following observation that even though it shields the passport against illegal data processing operations, it becomes inefficient in case of legitimate querying. Indeed, Faraday cages do not prevent eavesdropping on legitimate conversations between readers and tags. Nonetheless, they constitute an effective method for reducing the opportunity for unauthorised reading of the passport at times when the holder does not expect it.[184]
Furthermore, the relevance of these measures over time needs also to be asked. Indeed, some players have already voiced out concerns over the fact the cryptographic measures do not possess the desired long-term security (their validity is estimated to a maximum of 10 years).[185]

---

[178]Bundesamt für Sicherheit in der Informationstechnik, *Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents, Extended Access Control (EAC)*, Version 1.00, Germany, 2006.
[179] The zone that will be read is known as the Machine Readable Zone (MRZ). It is a special area of the passport.
[180] Pooters, 2008, pp. 5-6.
[181] Kc and Krager, "IBM Research Report", p. 6, cited in Bronk, 2007, p. 31.
[182] Witteman, M., "Attacks on Digital Passports", What the Hack Conference, Liempde, The Netherlands, 27 July 2005, cited in Bronk, 2007, p. 31.
[183] Meingast, et al., 2007, p. 38.
[184] Juels, A., D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports", in *Security and Privacy for Emerging Areas in Communications Networks,* 2005, p. 75 and 84.
[185] Buchmann, J., A. May, and U. Vollmer, "Perspectives for Cryptographic Long-Term Security," *Communications of the ACM*, Vol. 49, No 9, 2006, p. 54.

Finally, some e-passports' RFID chips do not store any personal information, but simply a code or serial number, which will be used by the reader to call up the relevant information that is stored in a database.[186] This might eventually be helpful in preventing skimming, but it is not able to counter other threats such as clandestine tracking (cf. *infra*, 3.2.2). Furthermore, this solution has the "defects of its advantages" because it entails storing vast amounts of highly sensitive personal information in a unique database. This is the very reason why some authors have recommended that biometric data is one of the rare cases where personal information should be stored on-tag.[187] The problem of storing the information either on-tag or within the database is particularly acute in the e-passport debate, given the biometric nature of the information to be stored.

3.4.2 Security threats/data processing operations that threaten the privacy

The very characteristics of the e-passport present new risks in terms of security, and hence privacy.
First, the RFID tags are permanently embedded in the passport, which in turn is an artifact that individuals are likely to carry with them in quite a big number of occasions, making the tag ever present or ubiquitous. This can be further dangerous if one keeps in mind that the data stored on the chip is static (some of it will never change), sensitive personal information (personal data such as name and address, but also biometric information). Third, the RFID nature of the passport may sometimes escape to the attention of the holder, and the latter may not be signalled that the RFID chip is being read, and by whom. Finally, because of the aforementioned characteristics, unauthorised reading may take place in public space, and without the holder knowing it.[188]

Because e-passports rely upon RFID technology, they present some risks that can be commonly found in many (if not all) RFID devices. However, they also feature specific risks.

From a privacy viewpoint, the security of RIFD systems is very important, and it can be argued that security and privacy are two faces of the same coin. Indeed, security flaws will allow for unlawful data processing operations, which will result with privacy threats for users.

Several security (and privacy) threats need be mentioned.

Unauthorised reading/scanning

Reading e-passports unauthorised can be undertaken through clandestine scanning. This threat is serious, especially in the light of the security and cryptographic weaknesses of the passport. Consequently, biometric passports can easily be subjected to short-range clandestine tracking (up to a few meters),[189] with the ensuing leakage of **biometric information** and of other personal data contained in the document.[190]

---

[186] van Lieshout et al., 2007, p. 197.
[187] Henrici, Dirk, 2008, p. 21; see also Hornung, G., *The European regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, 2007, p. 4. http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.asp
[188] Meingast, et al., 2007, p. 36.
[189] The range of the chip is purposefully limited to a few centimetres. However, it is possible to extend it up to a few meters with an appropriate device.
[190] Juels et al., 2005, pp. 76-78.

Clandestine tracking

Because the RFID standard for e-passport is a passive one (cf. ISO 14443), passports' tags will emit the ID chip on protocol initiation coming from any reader (since this operation does not require authentication). Since each passport carries a unique identifier, clandestine tracking is thereby made possible by reading this single information, storing it, and following its signal. This operation will enable the tracking of the RFID tag, and hence, of the individual carrying it.[191] Therefore, using the passport's unique identifier, it is possible to track the movements of the passport holder by repeatedly querying the passport.[192]

Cloning

Fourth, cloning of RFID can also happen, i.e., making an identical clone of the chip containing the passport information. The clone can be later used in place of the original, and without the user's knowledge.[193]

Skimming and Eavesdropping

Fifth, skimming and eavesdropping consists in the interception of the information contained in the chip, while the latter is communicating this information to an authorised reader.
Because of the aforementioned characteristics of the e-passport, the danger of these threats becomes more important. For instance, because of the permanent embeddedness of tags, the latter cannot be temporarily removed in order to avoid such threats.[194] Because of its passive nature, eavesdropping is particularly problematic.

Hotlisting

Hotlisting consists in building a database of all the available information concerning an individual, such that when an identifier is detected it can be linked to all the other information available concerning this particular individual.[195]

Back end system violations

It is important to keep in mind the structure of the RFID infrastructure. Personal information can either be read directly from the tag, or also from the back-end system.
Access to the database where the biometric and other personal information is stored also raises issues of privacy and data protection. The point here is less about the security of the tag, than of the protection of the databases where biometrical information might eventually be stored.

[191] Ibid.
[192] In practice, the use of a Faraday cage will make tracking very difficult or impossible. Indeed, it would only be possible to track the information when the Cage is open, that is, for legitimate querying operations. On the other hand, legitimate information retrieval operations will not solely take place in airports. This will be the case when checking in a hotel for instance. Although the information is not read through an electronic device, the passport needs still to be opened, and hence the Faraday cage as well.
[193] Ibid.
[194] Meingast et al., 2007, p. 39.
[195] Juels et al., 2005, p. 79.

3.4.3 Privacy violations

The different data processing operations that have been outlined above, will result in infringement upon the privacy of citizens. Determining how these practices infringe upon the privacy if citizens, or, in other words, determining what type of privacy is at stake by these operations, is the goal of the following section.

Concern of one's personal information to be accessed without one's knowledge and consent – being transparent.

People fear that some of their information might be continuously observed, without their permission or knowledge. They fear to be observed, permeated, and assessed without discontinuity, thereby becoming transparent. This implies that citizens want to have some control on the information that is read out (at distance) from them (or from their belongings, and that concerns either these belongings or themselves).[196] Citizens' autonomy is eroded as they have very little control on who is able to access their information that is contained into the RFID tags they are carrying.
This is maybe the biggest threat that results from the information security issues of the e-passport. Indeed, because of its security flaws, the e-passport makes it possible for unauthorised third parties to read the biometric information contained in the tag without the user's knowledge or consent. Hence, the latter can become totally transparent to individuals whose existence he is not even aware of.
This has raised fears among privacy advocates, as Bruce Schneier asserted that "Your passport information might be read without your knowledge or consent by a government trying to track your movements, a criminal trying to steal your identity or someone just curious about your citizenship."[197]

Concern for power inequalities

Because RFID systems allow for possibilities of non-stop observation and collection of data (cf. previous point), citizens also fear the consequences of such processes, i.e., the accumulation of data to which these practices lead might be used to accumulate knowledge about individuals.[198]
The fear is not only of becoming transparent to others (cf. previous point), but also the correlative consequence: the reader is opaque to the transparent person. There is therefore a fear of the power shift between the reader and the read.

But, not only are citizens afraid of power shifts, but also of the following operations that data processors can do with their information. In particular, the fear the reduced judgements that the actor in situation of superiority might make about them, and which would definitely categorize them without further possibilities of redemption. These very clear threats to autonomy can occur in situations of data mining and profiling.[199]

Concern to be followed (i.e., tracking)

[196] Spiekermann, 2008, p. 66.
[197] Schneier, 2006.
[198] Spiekermann, 2008, p. 67.
[199] Van Lieshout et al., 2007, p. 124; Meints and Gasson, 2009, p. 142.

Another use of their data being read that citizens fear is that object information can be read out and used to create movement profiles of their own whereabouts, since the latter could be deduced from the movements of the objects they own. This fear is not expressed in absolute terms however. According to a survey undertaken by Spiekermann, there are zones where citizens deem it legitimate to be tracked (i.e., in a shop), but as soon as the tracking concerns their "private territory" it becomes illegitimate to their eyes.[200] This can be understood as a violation of privacy of location and space.

Furthermore, *identity theft* is another risk.

3.4.4 Privacy and securities issues with the e-passport: some additional thoughts

In the preceding paragraphs, we have discussed the practices that threaten the security of the e-passport, and hence, the privacy of its users. These observations should trigger some reflexions on the desirability of the e-passport, at least in its current version.

Indeed, many observers and stakeholders have pointed out the fact that the whole process may have been rushed for reasons of political agenda, whilst the pace of technological progress may not yet have been appropriate.[201] Such a conclusions could be drawn from the fact that although compelled by the 2002 e-government act to undertake a full scale Privacy Impact Assessment regarding the implementation of the e-passport, the US government authored instead a PIA that fell well below the requirements, and that neither identified nor addressed issues of security and privacy triggered by the use of RFID technology.[202] In this respect, it is tempting to speculate over the influence the industry lobby has had over rational discourses on technical feasibility.[203]

But worse fears have also been raised as to the consequences of the inappropriateness of this technique, which may in fact not work and would at best provide no enhancement of identity and border control.[204]
One of the risks identified by Juels et al. is the overreliance upon automated authentication processes. This is already the case at the Kuala-Lumpur airport where Malaysians citizens present their e-passport to an "AutoGate" that identifies them without recourse to any human agency. If the fingerprints presented to the "AutoGate" match those contained in the e-passport, the gate opens and they are allowed forward. The lack of human oversight, especially in the light of the numerous existing threats might be perceived as facilitating the conditions for passport forgery and identity theft.[205]
From a biometrical point of view, the efficiency of resorting to identification through photographic characteristics remains very much disputed, and it poses many problems to say the very least.[206]
Moreover, even though governments decided to reconsider the security measures of the biometric passport after pressures from the civil society, the measures chosen are not the panacea. Indeed, we have seen above the many cracks and weaknesses both in the Faraday Cage

[200] Spiekermann, 2008, p. 68.
[201] Lipton, E., "Bowing to Critics, U.S. Plans to Alter Electronic Passports", *New York Times,* 27 April 2005. http://www.nytimes.com/2005/04/27/politics/27passport.html
[202] Meingast et al., 2007, p. 40.
[203] Bronk, 2007, p. 39.
[204] In darker scenarios, it might even further weaken the security of identification through passports. See, Bronk, 2007, p. 36.
[205] Juels et al., 2005, p. 79.
[206] Bronk, 2007, pp. 26-29.

and in the BAC. Plus, the American Department of Homeland Security has itself considered that the digital signature system used for encryption purposes could be potentially disastrous.[207]

More fundamentally, one can wonder whether RFID appears as the appropriate technology for purposes of e-ID, as well as the appropriateness of biometric technology for identification purposes. Indeed, because of the great risks that it presents, it remains questionable whether the benefits of using an electronic passport could have been obtained with a different technology than RFID. As the US Department of Homeland Security has written, "for applications related to human beings, RFID appears to offer little benefit when compared to the consequences it brings for privacy and data integrity. Instead, it increases risks to personal privacy and security, with no commensurate benefit for performance or national security."[208] This is especially true with regards to the RFID standards chosen, which are passive, and can be cracked more easily. In this respect, it is intriguing to notice that the security and encryption measures put in place require (e.g., BAC) require visual scans of the passports' data page in order to function correctly, thereby making one of the main advantages of the RFID passport (i.e., convenience and efficiency, especially at entry points) irrelevant.[209]

All in all, it seems that most of the promised advantages of the e-passport (i.e., better passport security, more convenience of use…) have been torpedoed by technical shortcomings, and dangers for the privacy and security of individuals. One can then wonder what exactly we have gained from the deployment of the e-passport, and it is maybe no wonder that, at the time of its deployment, qualified as a "loser system" by the journal of the largest US professional organisation of electrical engineering professionals and academics.[210]

3.5 EXTENT TO WHICH THE EXISTING LEGAL FRAMEWORK ADDRESSES THE PRIVACY IMPACTS

In this section we will try to determine whether the existing legal framework is able to cope with the privacy violations that can result from the use of RFID in the e-passport. Therefore, it is necessary to understand whether the data protection and privacy legal framework can effectively tackle the issues at hand (provided it applies to them), and whether new instruments are eventually needed.

Indeed, the e-passport can also be legally analysed as RFID devices that process very sensitive personal information (i.e., biometric data). In this respect EU legislation on privacy and data protection should apply to it.

The European framework for the protection of privacy and data protection is constituted of several instruments.

[207] Ibid. p. 37.
[208] Department of Homeland Security, Emerging Applications and Technology Subcommittee, *The use of RFID for human identification – version 1.0*, 2006.
[209] Meingast et al., 2007, p. 43.
[210] "Passport to Nowhere: the Radio-Tagged Biometric Passport Won't Faze Industrious Terrorists", *IEEE Spectrum*, January 2005, p. 55.

At Treaty level it is constituted of the Charter for Fundamental Rights, which protects both the right to privacy and data protection in its articles 7,[211] and 8.[212] Article 16 of the Lisbon Treaty also contains a general provision on the protection of personal data,[213] whilst article 8 of the European Convention of Human Rights of the Council of Europe protects the right to privacy.[214]

As far as data protection legislation is concerned, two Directives are concerned: Directive 95/46/EC known as the Data Protection Directive,[215] and Directive 2002/58/EC known as the e-privacy Directive.[216]

In other words, the issue at hand is the following one. In the preceding section, we have seen that the privacy of individuals can indeed be violated through the use of the e-passport. Interestingly enough, we have noticed that most of the potential privacy violations result from illegal data processing operations undertaken by third parties, the latter being made possible by the several security weaknesses of the device. In other words, what is at stake is an issue of information security, and the correlative privacy violations that may occur.
Therefore, the aim of this section is to determine whether the existing privacy and data protection legal framework is able to cope with these risks, and if not, what eventual changes would be required.

3.5.1 Applicability of the e-directive

As a preliminary point, we will examine the applicability of the e-privacy Directive, which is an application of the data protection principles to the electronic communication sector. Indeed, this Directive contains a provision on data breaches that can be of interest in the context of information security management. According to the Directive, a data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise pro-

[211] Article 7 of the Charter states that "Everyone has the right to respect for his or her private and family life, home and communications".
[212] Article 8 states that "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."
[213] Article 16 of the Lisbon Treaty states that "1.Everyone has the right to the protection of personal data concerning them. 2.The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."
[214] Article 8.1 states that: "Everyone has the right to respect for his private and family life, his home and his correspondence."
[215] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal,* L 281, Vol. 31, 23 Nov 1995, pp. 0031 – 0050.
[216] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal,* L 201, Vol. 45, 31 July 2002, pp. 0037 – 0047, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

cessed."[217] Furthermore, it is also provided that notification to individuals will be required if the data breach is likely to adversely affect their personal data or privacy, as in the case of identity theft.[218] The protection against data breaches is part of a broader obligation to guarantee the right to confidentiality of electronic communication networks, that is, ensuring they will not be eavesdropped, tapped, or whatsoever.[219]
Recital 56 of Directive 2009/136/EC of 25 November 2009 amending the e-privacy directive expressly provides that it applies to RFID,[220] as well as the article 3 of the amended Directive.[221]
However, and unfortunately, the scope of the e-privacy Directive remains very limited, as it applies solely to the processing of personal data in connection with the provision of publicly available electronic communication services in public communication networks. Consequently, the vast majority of the current FRID applications fall only under the scope of the Data Protection Directive, as RFID does not need to make use of a public available network in order to establish communication, and such is the case for the e-passport.[222]

Given the inapplicability of the e-privacy directive, one needs to turn towards the data protection directive, which is the cornerstone piece of legislation of the EU privacy and data protection legislative framework.

3.5.2 The Data Protection Directive

Applicability of the Directive

A preliminary question that needs to be answered is that of the applicability of the Directive.

Indeed, the Data Protection Directive solely applies to the processing of personal information, which according to its article 2(a), mean any information relating to an identified or identifiable individual. Hence the question as to whether the information carried on by RFID systems can qualify as personal data. As usual the answer will vary according to the type of data enshrined in a particular RFID tag.
In its opinion 4/2007, the Article 29 Working Party has attempted to clarify the situation.

The Working Party agrees that any information means both objective and subjective information, it includes any sort of information (e.g., family life, social conducts etc…), including so-called sensitive data (cf. art. 8 of the Directive). Also, the information can be of any format, such as graphical, alphabetical, or photographical data. Biometrics is also considered as personal information.[223]

---

[217] Article 2 (h).
[218] Article 4.3.
[219] Kruse, Andreas, Camino Mortera-Martinez, Véronique Corduant, Deutsche Post AG, Sebastian Lange and Pleon GmbH, "Work Package 5 – The Regulatory Framework for RFID", *CERFID project*, 2008, p. 45. www.rfid-in-action.eu/
[220] Recital 56 states that: "(…) When such devices [RFID are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply."
[221] Article 29 Data Protection Working Party, Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), WP 150, adopted on 15 May 2008, p. 5. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_en.pdf
[222] Kruse et al., 2008, p. 88.
[223] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data 4/2007, WP 136, 20 June 2007. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Furthermore, the information can relate to the individual either directly, or indirectly. Indirect personal information is especially important in the case of RFID, as in many cases, RFID tags do not contain personal information as such, but can nonetheless be linked to the individual behind the tag. Therefore, and following this distinction, the Article 29 Working Party considers that a data can relate to an individual, under three non-cumulative criteria have to be used: content, purpose, or result. Either the content of the data is about a person, either the information is not about a person but is used with the purpose of taking actions on this person, or either the information, although not about the person, can be used with an impact on this person.
As a matter of fact, the extent of what can be an identifier has to be examined on a case-by-case basis.[224]

In addition to this, the person needs to be identified or identifiable, that is, when, although the person is not identified yet, it is possible to do so.[225] In order to determine whether a person is identifiable or not, Recital 26 of the Directive provides that "*whereas to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller, or by any other person to identify the said person*."[226]
The criterion of all the means reasonable should take into account all the means that are concrete and not include a mere hypothetical possibility. Moreover, the Art.29 WP takes a pragmatic approach by stressing that this criterion should take all the factors at stake into account. This includes the cost of conducting the identification, the intended purpose, the way the processing is structured, the expected advantages, the interests at stake for the individual, the risks of organizational dysfunctions (e.g., breaches of confidentiality duty), and technical failures. Furthermore, the test should take into account the real-time level of technological development. Special importance must be given to the purpose of the data controller.[227]

In the case of RFID, the Art.29 WP distinguishes between tags containing personal information, tags storing information related to personal data, and tags that store "*non-traditional*" identifiers but that can potentially enable tracking and tracing of people. In addition, other types of tags might not contain personal information at all.
The biometric passport belongs to the first category, as the chip stores biometric data as well as information data. Even, when the tag contains only a unique identifier, the tag can always be combined with the back-end database where the personal information is stored. Therefore, it can be concluded that biometric passports fall under the Data Protection legislation.[228]

Data protection Principles

Given that the RFID applications enter indeed in the scope of the Data Protection Directive, it remains to be seen whether the principles contained therein can be instrumental in addressing the information security issues encountered earlier on.

Indeed, the Directive contains several milestone principles that have contributed to establish it as the benchmark data protection instrument.

[224] Ibid., p. 12.
[225] Ibid.
[226] Emphasis ours.
[227] Article 29 Data Protection Working Party, *op. cit.*, 2007.
[228] Ibid.; Kruse et al., 2008, pp. 76-78.

First, there are the principles concerning the manner in which the processing must be conducted: they include the purpose specification principle, and the data quality principle.[229]
Second, there are the legal grounds for processing. The processing of personal data will be deemed as legitimate insofar as it meets one of the legitimate processing aims laid down in article 7 of the Data Protection Directive, mainly, either the realisation of a legitimate aim pursued by the data controller, either the data subject has given his/her free and unambiguous consent.[230]
Third, the Data Protection Directive grants different subjective rights to data subjects, amongst which, the right to be informed, to access the data, to rectify it, and to object the processing.[231]
Finally, security of the processing must be guaranteed through appropriate technical and organisational measures.[232]

The question is therefore the following one: would the application of the relevant provisions of the data protection directive be able to mitigate the security flaws. Answering this question entails answering the following question: can the Directive and its principles be applied to RFID applications, and if so, how?

Indeed, as part of the ICT revolution, RFID have come along with a new set of technology deriving risks, which the current legal framework had not foreseen at the time of its entry into force. Therefore, and although the principles contained in the data protection directive are still valid, the fact remains that there are some gaps in the actual legal framework as to its applicability to RFID applications.[233]

---

[229] Article 29 Data Protection Working Party, Working Document on data protection issues related to RFID technology, WP 105, 19 Jan 2005, p. 9. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf

[230] See Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Oxford, 2002, pp. 98-99. Article 7 states that: "Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

[231] Art. 10, 11, 12.

[232] Art. 17.

[233] See, Article 29 Data Protection Working Party, 2005, p. 2; EDPS, Opinion on promoting trust in the Information Society by fostering data protection and privacy, 18 March 2010, p. 2. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf See also, Article 29 Data Protection Working Party and Working Party on Police and Justice, The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 Dec 2009, p. 12. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf: "*The basic concepts of Directive 95/46/EC were developed in the nineteen seventies, when information processing was characterized by card index boxes, punch cards and mainframe computers. Today computing is ubiquitous, global and networked. Information technology devices are increasingly miniaturized and equipped with network cards, WiFi or other radio interfaces. In almost all offices and family homes users can globally communicate via the Internet. Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects*." It goes on then to say that "*Directive 95/46/EC has stood well the influx of these technological developments because its principles and concepts remain relevant, valid and applicable in today's networked world*." Nonetheless, "*While it is clear that technological developments described above are generally good for society,*

As the EDPS puts it, the new ICT environment creates new risks and new concerns that are not accounted for within the existing legal framework. Therefore, it has argued that specific measures and legislations are necessary in order to implement the right and principles of data protection legislation at RFID level.[234]

Furthermore, the EDPS retains that the existing EU legal framework concerning RFID, although relevant, contains nonetheless several gaps as far as privacy safeguards are concerned. The legislation is not sufficiently detailed to cope with the new privacy challenges raised by this technology.[235]

In other words, the recent developments of ICTs, and in particular of RFID, have led to the emergence of new risks for the privacy of individuals, which threaten the effectiveness of the legislative framework. Therefore, and in order to adequately apply the yet relevant data protection and privacy principles, legislative change is needed. Such a change would create the opportunity to clarify key rules and principles (e.g., consent and transparency), or to innovate the framework by enriching it with additional principles/implementation provisions.[236] The existing principles need to be endorsed, and complemented with measures to execute these very principles in an effective manner.[237]

3.6 NEED FOR NEW LEGISLATION, CODES OF CONDUCT, ETC.

Departing from these observations, several key institutional stakeholders have adopted guidelines, recommendations, opinions, etc. in order to actuate the legal framework to the privacy risks and threats presented by RFID applications.[238]
Most players agree that what is required is to further detail the existing legislation by complementing it with additional rules imposing specific technical safeguards against new risks. On the other hand, it is also acknowledged that technology-specific regulation is also necessary.[239] These non-binding guidelines therefore contain principles that should guide the legislative process to come, which means that the best practices contained therein should be understood as first yet not complete indications on how to apply the legislative framework to RFID.

The following paragraphs will build upon the different document and guidelines in order to see, first, how the data protection principles can be best made relevant within RFID systems, and second, how technological tools might better implement these principles, and address some of the security risks.[240]

---

nevertheless they have strengthened the risks for individuals' privacy and data protection. To counterbalance these risks, the data protection legal framework should be complemented."
[234] EDPS, 2010, pp. 2, 11-12.
[235] Ibid., p. 11.
[236] Article 29 Data Protection Working Party and Working Party on Police and Justice, 2009, p. 6.
[237] Ibid., pp. 7-8.
[238] See for example, European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final, 12 May 2009. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf; EDPS, 2010; Article 29 Data Protection Working Party, 2005; 2007; 2008; 2009.
[239] EDPS, 2010, p. 11; Article 29 Data Protection Working Party, 2009, p. 12.
[240] Article 29 Data Protection Working Party, 2005, sections 4 and 5.

As far as consent is concerned, and although some authors consider it of secondary importance in respect to the legitimate aim principle,[241] it appears that, according to the Art.29WP, "*under most of the scenarios where RFID technology is used, consent from individuals will be the only legal ground available to data controllers to legitimise the collection of information through RFID*".[242] However, the Working Party also acknowledges that, ultimately, the appropriate legitimating ground will depend on the specific circumstances of each processing.[243]
As far as the e-passport is concerned, one might indeed argue that it could rely on article 7(e), i.e., the situation whereby the "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." If the ground of consent was to be retained, several problems would spur, since, according to article 2(h), the consent shall be freely given, specific (for the purpose the data are collected), and "*unambiguous*".
For RFID applications storing personal data on the tag, or having for purpose the identification of persons (as is thus the case for e-passports), the data subjects are, in practice, generally asked to give their consent explicitly.[244] This raises issues as to the validity of users' consent. Indeed, the level of awareness concerning the existence of an RFID chip in e-passports is quite low, which implies they cannot give a fully unambiguous consent. Moreover, in the case of the e-passports citizens have no choice whether to use it or not as its use results from a public obligation: if they want to travel, they need to use the RFID integrated passport.[245]

As far as the right to be informed is concerned, the following information must be provided to data subjects: identity of the controller, the purposes of the processing as well as, among others, information on the recipients of the data, and the existence of a right to access. Finally, it is important to state that one of the most important aims of disclosing this information is to put the data subject in a situation wherein he fully understands the effects of the RFID application.[246] However, in the light of the security threats of the e-passport these measures are of little help. Indeed, passport control is in general well indicated, and informing users about unlawful processing seems a bit paradoxical.
The data subject's right to access allows the latter to checking the accuracy of the data processed, and to ensure that the data are kept up to date.[247]

These rights can be better implemented through technical provisions, which are foreseen by article 17 of the Directive. Article 17 stipulates that the security of the processing must be guaranteed through appropriate technical and organisational measures. It can be considered to some extent as the cornerstone provisions in matters of security, as it imposes an obligation upon the data controller to implement the appropriate measures to protect personal data against accidental destruction or unauthorised disclosure.[248] However, article 17 needs too to be further detailed with respect to the latest ICT evolutions.

---

[241] See Gutwirth, 2002, pp. 100-101.
[242] Article 29 Data Protection Working Party, 2005, p. 10.
[243] Ibid., see in particular footnote 11 of this chapter.
[244] Kruse et al., 2008, p. 83.
[245] Article 29 Data Protection Working Party, 2009, p. 17.
[246] Article 29 Data Protection Working Party, 2005, pp. 10-11.
[247] Ibid. p. 11.
[248] Ibid. Equally, article 14.3 of the e-privacy directive contains a similar provision, although explicit reference to it has never been made yet, see EDPS, 2010, p. 7. Article 14.3 states that: "Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications."

Therefore, article 17 can be understood both as the provision concerning both the implementation of security safeguards, and the implementation of technical measures, the aim of which being the adequate application of the other data protection principles.[249]
Privacy by Design is seen as the major technical solution in order to adequately implement article 17.[250]
The idea behind Privacy by Design (PbD), is to design data processing devices (in our case, RFID) so as to best comply with data protection requirements: by incorporating privacy enhancing techniques *a priori*, most of the issues that might be raised by a given technology could be addressed.[251] Recital 46 of the data protection directive acknowledges the need for technical solutions, which must be applied as early as possible.[252] Also, linked to the concept of PbD is the notion of "Privacy Enhancing Technologies" (PETs), which are "ICT measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system."[253]

PbD and PETs can provide solutions in order to better implement from a technical viewpoint the principles of the data protection directive.
As already outlined previously the transparency of the processing is a crucial element in the security of the e-passport. Therefore, several ways of implementing the right to information have been put forward, such as the use of pictograms signalling the presence of RFID readers or tags has been suggested as being an important element in preventing the unauthorised gathering and reading of data through RFID technology. Equally, the real activation of tags is a step towards this direction.[254] Those are of course merely suggestions, and there is a need for a new legal framework with clearer and tailor made solutions.[255] In addition, individuals should be notified when a privacy breach occurs, as it will most probably affect their privacy.[256]

Implementing the right to access, content rectification, and content deletion will be done mainly through a so-called "kill command", which can permanently or temporarily deactivate the tag. However, this solution still presents some hurdles like reactivation difficulties, or the impossibility to implement it in all kinds of tags.[257] Consequently, other solutions have been put forth, such as using a clipping antenna, or overwriting the data placed on the data. However they are not without problems too.[258]
Furthermore, the possibility to disable tags can also be used in the context of consent when it is used as the ground legitimizing the processing. Consent is often understood, at least in the retail sector, as the possibility to deactivate the tag. Two ways of proceeding are possible: opt-in (standard deactivation) and opt-out (deactivation on request). In other words, the data subject will give his/her explicit and active consent for a RFID application by either resorting to

[249] Kruse et al., 2008, pp. 87-88.
[250] Article 29 Data Protection Working Party, 2005; Kruse et al., 2008, p. 89.
[251] Kruse et al., 2008, p. 90.
[252] Recital 46 states that the technical measures need to be "be taken both at the time of the design of the processing system and at the time of the processing itself."
[253] European Commission, Communication on promoting Data Protection by Privacy Enhancing Technologies; COM(2007) 228 final, 2 May 2007.
http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf; EDPS, 2010, *op. cit.*, p. 8.
[254] Article 29 Data Protection Working Party, 2005, p. 14.
[255] Article 29 Data Protection Working Party, 2009, op. cit., p. 16.
[256] Ibid.
[257] Article 29 Data Protection Working Party, 2005, p. 15.
[258] Kruse et al., 2008, pp. 92-93.

devices that automatically deactivate the RFID tag unless the data subject chooses otherwise, or by letting the tag activated unless the data subject chooses to deactivate it.[259]
In the retail sector, the opt-out solution has been so far retained. In the context of the e-passport however, the opt-in solution seems more appropriate, provided it overcomes the technical hurdles that still remain. However, the opt-in solution seems more appropriate to the e-passport.
Finally, and as far as data breaches (or data security) are concerned, the Art.29 WP proposes two types of measures: encryption and authentication. Encryption is the technique used in cryptography for making information indecipherable to anyone except for those possessing the right key, i.e., a special knowledge that transforms the encrypted information into usable information. It is therefore used in the RFID context in order to prevent unauthorised access to the information stored into the tag. In the framework of the e-passport, this is done through the BAC. However, the weaknesses of the process have already been evidenced earlier on. Another technique is authentication, that is, the authentication of the reader. This is also done through the BAC, and suffers the same criticism.[260]
On the other hand, article 17 of the data protection directive mentions organisational measures to be taken as well. These measures include mainly Privacy Impact Assessments (PIAs). That is, a study on the potential privacy implications that an application may have.[261] As a matter of fact, the European Commission has issued several recommendations for a PIA RFID framework.[262] The Article 29 WP has undertaken a large-scale industry consultation in 2005, and in 2011 it has issued recommendations based on a revised proposal submitted by industry for a privacy and data protection impact assessment framework for RFID applications.[263]

3.7 PRIVACY LEGISLATION AND RFID, WHAT CONCLUSIONS?

So far, we have analysed ways in which the existing privacy and data protection framework can apply to RFID applications, and in particular, the e-passport.

Again, the issue at stake here is **privacy violations that result from issues of information security** within the e-passport.
Most of these security issues come from the constant evolution of ICTs, of which RFID is an important part. Therefore, and as pointed out above, data protection and privacy legislation should be implemented in a way that is able to cope with these issues. This requires complementing these texts with provisions on information security management.[264]
In the preceding paragraphs we have described some of the most relevant propositions to adequately adapt the legal framework.

Several conclusions can be drawn from these observations.
It appears that many of the measures described deal with user empowerment. Indeed, be it measures concerning the rights to access, rectification, erasure, or consent, the data subject is "put at the centre of the game." This approach is coherent with the opinion of the Art.29

[259] Ibid., pp. 83-84.
[260] Ibid., p. 97.
[261] Ibid., p. 95.
[262] European Commission, Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, (2009/387/EC), Official Journal of the European Union, L 122, 16 May 2009, pp. 47-51.
[263] Article 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, 11 February 2011.
[264] European Commission, 2009, p. 4.

WP,[265] or with that of the EDPS.[266] The role of the data subject is enhanced through increased transparency, and a more heavily weighted consent. Furthermore, these provisions should be better implemented thanks to the technical and organisational measures of art.17 of the Data Protection Directive. PbD and PETs contribute to the security of RFID systems in a two-folded fashion. First, they are technical solutions that enable for the implementation of the provisions that adapt data protection legislation to RFID. Second, they increase the security of RFID systems by making possible the implementation of security measures such as cryptography or authentication.

One has to wonder therefore, whether this legislative framework is able to cope with the privacy threats identified earlier on in this document.

For example, some of the proposed technological solutions are difficult to implement, in general, and specifically in the case of the e-passport. This is the case for "kill commands", or other measures enforcing the right to be informed. The recommended encryption measures have already been implemented in the e-passport, however, they have not proven to be efficient. As previously evidenced, when pushing for the adoption of the document, the US government rushed the PIA process that consequently fell below any acceptable standards; PbD was largely absent of the crafting process, which might explain its important vulnerability to security threats; and the encryption technique used after pressures from privacy advocates has also shown its limitations. Second, some of these observations have been made from a general RFID viewpoint, which entails that they may be valid for some applications but not for all of them (e.g., retail applications would retain the opt-out solution, but for e-passports opt-in may be more appropriate). This was very clear as far as issues of consent are concerned, where guidance for the retail sector cannot be transposed mutatis mutandis to the e-passport.
This leads us to the fact that there is a need for technology-specific, tailor made legislation, which is non-existent to this day. Some explanation may be found in the fact that many aspects of the biometric passport remain under the competence of member States. However, that is not the case for the RFID aspects of the passport, and in particular, the security of this technology. Moreover, this is consistent with the several recommendations analysed above. And finally, the lack of specific legislation constitutes a problem from another viewpoint: that of the binding character of the recommendations, opinions, and communications analysed so far. Indeed, since all these documents have no actual binding force, they can only be used from the point of view of self-regulation. This is the reason EDPS advocated for a binding provision on PbD in the revised data protection directive, and for other similar comments of the art.29 WP.

As a conclusion, as a RFID device, the e-passport is confronted to the next generation of information risks that have come to the fore along with the development of ICTs.
In its current state, the legal framework is not in a position to address all these security and ensuing privacy issues, although it has the potential to. There is a need for new binding regulation that would determine how to best implement the data protection principles to RFID devices, and in particular, that would address the information risks born from this technology.

[265] Article 29 Data Protection Working Party, 2009, pp. 6, 15-16.
[266] EDPS, 2011.
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

3.8 REFERENCES

Acuity Market Intelligence, *ePassport Market Adoption to Reach 88% by 2014*, 2011. http://acuity-mi.com/PR%20GePPeV%202.pdf

Article 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, 11 February 2011.

Article 29 Data Protection Working Party and Working Party on Police and Justice, The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 Dec 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf:

Article 29 Data Protection Working Party, Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), WP 150, adopted on 15 May 2008. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_en.pdf

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data 4/2007, WP 136, 20 June 2007. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 Data Protection Working Party, Working Document on data protection issues related to RFID technology, WP 105, 19 Jan 2005. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf

Avoine, Gildas, Kassem Kalach, Jean-Jacques Quisquater, *"E-passport: Securing International Contacts with Contactless chips", Lecture Notes in Computer Science, Vol. 5143, 2008.*

BBC News, "ID card scheme 'to cost £5.6bn'", 8 Nov 2007. http://news.bbc.co.uk/2/hi/uk_news/politics/7084560.stm

Bronk, Christopher, *Innovation By Policy: A Study of the Electronic Passport*, 2007, pp. 4-7. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1557728

Buchmann, J., A. May, and U. Vollmer, "Perspectives for Cryptographic Long-Term Security," *Communications of the ACM*, Vol. 49, No 9, 2006.

Bundesamt für Sicherheit in der Informationstechnik, *Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents, Extended Access Control (EAC)*, Version 1.00, Germany, 2006.

Department of Homeland Security, Emerging Applications and Technology Subcommittee, *The use of RFID for human identification – version 1.0*, 2006.

Espiner, Tom, "IBM, CSC win ID card biometrics contracts", *ZDNet*, 7 April 2009. http://news.zdnet.co.uk/security/0,1000000189,39637650,00.htm

European Commission, Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, (2009/387/EC), *Official Journal of the European Union*, L 122, 16 May 2009, pp. 47-51.

European Commission, Communication on promoting Data Protection by Privacy Enhancing Technologies; COM(2007) 228 final, 2 May 2007. http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf

European Commission, Radio Frequency Identification (RFID) in Europe: Steps towards a policy framework, COM(2007)96 final, 15 Mar 2007.

European Commission, Decision K (2005) 409 of 28 February 2005. http://europa.eu.int/comm/justice_home/doc_centre/freetravel/documents/doc/c_2005_409_fr.pdf.

European Commission, Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued

by Member States, *Official Journal of the European Union, L 385, Vol. 37, 29 Dec 2004, pp. 0001 – 0006.*

European Commission, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal of the European Union,* L 201, Vol. 45, 31 July 2002, pp. 0037 – 0047.

European Commission, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Union,* L 281, Vol. 31, 23 Nov 1995, pp. 0031 – 0050.

European Commission, Joint Research Centre, Security Technology Assessment Unit. http://sta.jrc.ec.europa.eu/index.php/technical-challenges-for-identification-in-mobile-environments

European Data Protection Supervisor (EDPS), Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", 2011. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

EDPS, Opinion on promoting trust in the Information Society by fostering data protection and privacy, 18 March 2010. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf

Finkenzeller, Klaus, *The RFID Handbook – Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, third edition, Wiley, Chichester, 2010.

Gipp, Béla, Jöran Beel, and Ivo Rössling, *ePassport: The World's New Electronic Passport*, 2007. www.epassport-book.com

The Guardian, "Cost of ID card and passports rises to £100", 9 Nov 2007. http://www.guardian.co.uk/uk/2007/nov/09/idcards.politics.

The Guardian, "Cost of ID cards rockets by £840m", 10 May 2007. http://www.guardian.co.uk/politics/2007/may/10/idcards.immigrationpolicy

Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Oxford, 2002.

Henrici, Dirk, *RFID Security and Privacy – Concepts, Protocols, and Architectures*, Springer, Berlin, 2008.

Hoepman, Jaap-Henk, Engelbert Hubbers, Bart Jacobs et al., "Crossing Borders: Security and Privacy Issues of the European e-Passport", in Yoshiura, Hiroshi, Kouichi Sakurai et al. (eds.), *Advances in Information and Computer Security. Proceedings of the First International Workshop on Security*, IWSEC 2006 Kyoto, 23-24 Oct 2006, Springer, Berlin, 2006.

Hornung, G., *The European regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, 2007. http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.asp

IEEE Spectrum, "Passport to Nowhere: the Radio-Tagged Biometric Passport Won't Faze Industrious Terrorists", January 2005.

International Civil Aviation Organisation (ICAO), *Technical Report – Biometrics Deployment of Machine Readable Travel Documents*, Version 2.0, 2004.

Ivantysynova, Lenka, Ziekow, Holger, “RFID in Manufacturing: From Shop Floor to Top Floor, in Günther, Oliver, Wolfhard Kletti and Uwe Kubach (eds.), *RFID in Manufacturing*, Springer, Berlin, 2008.

Juels, A., D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports", in *Security and Privacy for Emerging Areas in Communications Networks,* 2005.

Kruse, Andreas, Camino Mortera-Martinez, Véronique Corduant, Deutsche Post AG, Sebastian Lange and Pleon GmbH, “Work Package 5 – The Regulatory Framework for RFID”, *CERFID project*, 2008. www.rfid-in-action.eu/

Le Point, “Gemalto”, 25 September 2008. http://www.lepoint.fr/archives/article.php/277010

Le Point, “Le prix des passeports pourrait augmenter”, 3 Oct 2008. http://www.lepoint.fr/archives/article.php/279393; Le Point, “Le passeport biométrique, une manne pour l’État”, 1 July 2010. http://www.lepoint.fr/societe/le-passeport-biometrique-une-manne-pour-l-etat-01-07-2010-1209696_23.php

Lipton, E., “Bowing to Critics, U.S. Plans to Alter Electronic Passports”, *New York Times,* 27 April 2005. http://www.nytimes.com/2005/04/27/politics/27passport.html

Meints, Martin, and Mark Gasson, “High-tech ID and Emerging Technologies”, in Rannenberg, Kai, Denis Royer and André Deuker (eds.), *The Future of Identity Systems in the Information Society – Challenges and Opportunities*, Springer, London, 2009.

Pooters, I., *Keep out of My Passport: Access Control Mechanisms in E-passports*, 2008. http://www.avoine.net/rfid/

PR Newswire Europe, “L'Etonie retient Gemalto pour sa solution de passeport électronique”, 2011. http://www.prnewswire.co.uk/cgi/news/release?id=182028

Schneier, Bruce, “The Id Chip You Don’t Want to see in Your Passport”, *The Washington Post*, 16 Sept 2006.

Spiekermann, Sarah, *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*, Shaker Verlag, Aachen, 2008.

US Congress, Enhanced Border Security and Visa Entry Reform Act of 2002, Public Law 107-173, 107th Congress, 2nd Session, 14 May 2002.

van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij and Claudio Borean, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, Office for Official Publications of the European Communities, Luxembourg, 2007.

Chapter 4, Privacy, Data Protection and Ethical Concerns in relation to New Technologies of Surveillance:

Whole Body Imaging Scanners and Unmanned Aircraft Systems

Rachel Finn and David Wright
Trilateral Research & Consulting, LLP

4.1 INTRODUCTION

This report seeks to identify the ethical, privacy and data protection concerns surrounding the use of new surveillance technologies in Europe. The report focuses on two micro-case studies, whole body imaging scanners and unmanned aircraft systems (UASs), both of which have newly emerging civil applications. Hundreds of whole body imaging scanners are currently deployed in airports in the USA, Europe, Canada, Nigeria and Russia, while still further countries are conducting trials or considering their use. Significantly, this deployment of whole body scanners has raised significant controversy around the world in relation to privacy, data protection and ethics. In contrast, the use of UASs has generated significantly less debate around privacy and data protection, despite a slow increase in the introduction of UASs in civil applications, such as law enforcement, border patrol and other regulatory surveillance. This report analyses the current deployments of these technologies and the stakeholders who are involved, and explores the ethical, privacy and data protection issues that these technologies raise. It also examines whether existing ethical principles and legal regulations are valid and applicable for these technologies and what sorts of rules could and should be implemented in the future to ensure the right to privacy.

4.2 METHODOLOGY

In order to assess the impacts of new technologies of surveillance on privacy, both micro-case studies presented here will analyse six issues. These include:

1. the current status-quo of such technologies;
2. the set of academic, industrial and state actors that are driving their development, and their intentions;
3. possible users or beneficiaries;
4. possibilities for privacy-infringing uses and practices;
5. the extent to which existing ethical principles and legal regulations are valid and applicable for new surveillance technologies;
6. possible pathways for future oriented new ethical rules and regulations to ensure the right to privacy.

In order to address these issues, we have undertaken a literature review of academic articles, research reports, newspaper articles, legal materials and web materials that discuss the capabilities, uses, privacy concerns and regulatory regimes of these new technologies.

4.3 BODY SCANNERS, SECURITY AND PRIVACY

4.3.1 Introduction

Although the attempted bombing of an Amsterdam to Detroit flight in 2009 is often cited as the beginning of the deployment of whole body imaging scanners, principally at airports, the systems and technologies used to develop and deploy these scanners originated in the mid-1990s. These systems seek to address the fact that current technologies and screenings, such as walk-through metal detectors and hand searches, have deficiencies in detecting some types

of threats, and law enforcement and security staff need tools to enable them to deal with threats from explosives and non-metallic weapons.[267]

Whole body imaging scanners, or body scanners, provide one possible means of reducing the threat from non-metallic weapons. Body scanners "produce an image of the body of a person showing whether or not objects are hidden in or under his clothes" by using x-ray backscatter or millimetre waves.[268] Given the sensitive nature of the images produced by body scanners, a number of privacy concerns have been raised in relation to their mass deployment, particularly at large airports, and a number of policies and procedures have been implemented to address these privacy concerns. However, a comprehensive, international agreement on standards, policies and procedures that would provide robust protections for those who may be subject to body scanning technologies, whilst simultaneously protecting the travelling public from the threats body scanners are intended to address, has yet to be agreed. This report reviews these debates and analyses future-oriented policies that would provide such robust protection.

4.3.2 Current status of the technology and expected progress in the near future

Three different types of body scanning technologies are available on the market today. These include x-ray backscatter scanners, active millimetre wave scanners and passive millimetre wave scanners. Each of these systems uses the distinctions between the chemical components of a human body and other substances to detect when an individual is carrying concealed weapons on their person. For example, L-3 Communications, the makers of the ProVision millimetre wave scanner assert that their scanner can identify:

> objects made of any material, including liquids, rubber, wire, plastic, and metal, to quickly and easily locate weapons, contraband, and other threats concealed under an individual's clothing. The portals detect concealed and hidden objects such as metallic and non-metallic weapons and virtually all known explosives, and other contraband in seconds.[269]

If suspicious objects are identified, the individual is required to undergo a physical pat-down to identify any objects the person might be carrying.[270]

The most common type of body scanner is those that use X-ray backscatter, which work by comparing the density of different types of materials and highlighting inconsistencies. According to Demetrius Klitou, "Objects with a high atomic number (high Z materials), such as metallic weapons, absorb X-rays, while explosives, containing, for example, nitrogen and carbon, which have a low atomic number (low Z materials), scatter X-rays."[271] As individuals stand inside a portal, low dosages of X-rays are beamed towards them and pass through their

---

[267] Venier, Sylvia, "Global Mobility and Security", *Biometric Technology Today*, May 2010, pp. 7-10.

[268] European Commission, Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, Brussels, 19 Feb 2009. http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm

[269] L-3 Communications, "TSA to Test L-3 Millimeter Wave Portals at Phoenix Sky Harbor Airport", press release, 11 Oct. 2007. http://www.l-3com.com/news-events/pressrelease.aspx?releaseID=1061924

[270] Department of Homeland Security, *Privacy Impact Assessment for TSA Whole Body Imaging*, 17 Oct 2008, p. 3. http://epic.org/privacy/body_scanners/DHS_PIA_08_17_08.pdf. DHS published an update, 23 July 2009. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbiupdate.pdf. Another updated appeared 25 Jan 2011. http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf

[271] Klitou, Demetrius, "Backscatter body scanners – A strip search by other means", *Computer Law & Security Report*, Vol. 24, Issue 4, 2008, pp. 316-325 [p. 317].

clothes. The pattern in which they are "scattered back" once hitting an individual's body reveals an image of the person. "Concealed objects, both metallic and non-metallic, are distinguishable in backscatter images due to their significant differences in atomic number from human tissue. The image edges of concealed objects of low Z material are automatically enhanced to facilitate their detection".[272] Some X-ray systems, such as the Rapiscan single pose, offer simultaneous front and back scanning to eliminate "blind spots and potential opportunities for concealment"[273].

In an active millimetre wave scanner, individuals step inside a machine that resembles an "over-sized telephone booth with open sides".[274] Two antennas transmit and receive high-frequency radio waves as they circle the individual. The waves pass through clothing but bounce off materials such as skin and concealed objects. Very high-density materials such as metal will reflect more energy than human flesh,[275] and this raw, reflected data is transformed into a 3-D image of the individual with "some surface detail of the body".[276] Passive millimetre wave scanners work similarly, although they form an image from the "natural millimetre-wave radiation emitted by the body, or reflected from the surroundings" and "produce rough and blurred body images [while] concealed objects, metallic and non metallic, (particularly the larger ones) prove to be clear".[277]

Although there are concerns about the safety of both x-ray and millimetre wave body scanners, particularly for children, pregnant women and those with disabilities or fragile immune systems, these systems have been judged safe for use on people. The European Commission states that the dosage one experiences from backscatter x-rays is equivalent to "2% of the dosage of radiation experienced by a passenger during a long-haul flight", while millimetre wave scans are "equivalent to 0.01% of the permissible dosage for mobile phones".[278] Furthermore, unlike x-ray scanners, the high-frequency radio waves emitted by millimetre wave scanners do not pose any potential for tissue damage[279] and passive millimetre wave scanners do not emit radiation[280]. Some of these systems also incorporate privacy enhancing technology (PET) elements, such as remote operator work stations or software filters that blur sensitive areas of the body[281].

Sites of application

Body scanners are being used in a number of locations and for a range of purposes; however, it is primarily their deployment at airports that is generating attention and controversy. The deployment of body scanners in airports has primarily been concentrated in the USA, but

[272] Ibid.
[273] Rapiscan Systems, "Backscatter / Rapiscan Secure 1000 Single Pose", 2011. http://www.rapiscansystems.com/rapiscan-secure-1000-single-pose.html
[274] Clark, Pilita, "How airport body scanners will be used", *Financial Times*, 30 Dec 2009. http://www.ft.com/cms/s/0/4c4887ec-f594-11de-90ab-00144feab49a,dwp_uuid=f39ffd26-4bb2-11da-997b-0000779e2340.html
[275] Conroy, Michael, "How the ProVision 'naked airport scanner' works", *Wired.co.uk*, 14 May 2010. http://www.wired.co.uk/magazine/archive/2010/06/start/how-the-provision-naked-airport-scanner-works
[276] European Commission, Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports COM(2010) 311/4 , Brussels, 2010, p. 8.
[277] Ibid. , p. 7-8.
[278] European Commission, op. cit, 2009, p. 1-2.
[279] Conroy, op. cit., 2010.
[280] European Commission, op. cit., 2010, p. 8.
[281] Rapiscan Systems, "Backscatter / Rapiscan Secure 1000 Dual Pose", 2011. http://www.rapiscansystems.com/rapiscan-secure-1000.html

some European countries have also installed them, and non-western countries are beginning to trial them or consider their use.

The deployment of body scanners in airports in the USA is difficult to pin down as numbers are continually increasing. Early trials of L-3 and Rapiscan systems occurred in Phoenix Sky Harbor Airport and Chicago O'Hare Airport respectively in 2007. In December 2009, L-3 communications reported that more than 200 of their ProVision Millimeter Wave scanners were deployed worldwide, including "40 systems at 19 [US] airports" as well as "other facilities that include federal and state courthouses, correctional institutions, embassies and border crossings."[282] The TSA's website claims that there are currently 486 scanners at 78 US airports[283], and Kravitz of *The Washington Post* reports that "by the end of next year, 1,000 X-ray machines will be operational, accounting for roughly half of the nation's 2,000 lanes of security checkpoints"[284] At some airports, the machines are being used for "primary screening" in that passengers can choose to go through scanners instead of going through traditional metal detectors, but in many cases, machines are being used for "secondary screening" where they screen passengers who have set off the metal detectors.[285] But the US plans to gradually introduce body scanners as primary screening mechanisms and plans to increase the number of body scanners deployed to 1,800 by 2014.[286]

Airports in the European Union represent another major site of body scanning technology. Schiphol airport in Amsterdam became one of the first major international airports to introduce body scanners in May 2007.[287] Rapiscan x-ray backscatter systems have also been deployed at Manchester Airport and London's Heathrow Airport since February 2010. Unlike deployments in American airports, those who are subject to body scanners in UK airports are not able to request a physical pat-down search instead of a body scan, and the UK government has said that "passengers who refuse to go through an airport body scanner will be refused permission to fly".[288] Hamburg Airport began a six-month trial of two body scanners in September 2010, and passengers in Hamburg can choose whether to go through normal security or bypass security with a body scan.[289] France has begun a three-year trial of body scanners in "areas of airports not freely accessible to the public" in Paris Roissy and Charles de Gaulle airports.[290] *Jaunted* web-magazine has also reported the use of body scanners in Rome's Leo-

[282] *airport-technology.com*, "TSA Approves L-3's ProVision Millimeter Wave Checkpoint Screening System", 4 Dec 09. http://www.airport-technology.com/contractors/security/l-3_security/press35.html
[283] Transportation Security Administration, "Advanced Imaging Technology (AIT)", 2011. http://www.tsa.gov/approach/tech/ait/index.shtm
[284] Kravitz, Derek, "Are airport X-ray machines catching more than naked images?", *The Washington Post*, 26 Dec 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/12/25/AR2010122502277.html?hpid=topnews
[285] Associated Press, "Dutch to use full body scanners for U.S. flights", *MSNBC.com*, 30 Dec 2009. http://www.msnbc.msn.com/id/34630097/ns/us_news-airliner_security/
[286] European Commission, op. cit., 2010.
[287] United Press International (UPI), "Airliner attack re-ignites scanner debate", 29 Dec 2009. http://www.upi.com/Top_News/Special/2009/12/29/Airliner-attack-re-ignites-scanner-debate/UPI-98181262114910/
[288] Millward, David, "Passengers who refuse scanner face flying ban", *The Telegraph*, 1 Feb 2010. http://www.telegraph.co.uk/travel/travelnews/7129835/Passengers-who-refuse-scanner-face-flying-ban.html
[289] Privacy International, *Germany - Privacy Profile*, 26 Jan 2011. https://www.privacyinternational.org/article/germany-privacy-profile
[290] Privacy International, *France - Privacy Profile*, 22 Jan 2011. https://www.privacyinternational.org/article/france-privacy-profile

nardo da Vinci airport[291] and L-3 Communications report the use of their body scanners in Madrid Barajas International Airport[292]. Yet not all EU countries are considering the deployment of body scanners. Privacy International reports that the Norwegian Aviation Authority, Avinor, proposed the use of body scanners as airport security measures; however, strong negative reaction from the public resulted in a cancellation of the proposal.[293]

Other countries are also using or considering the use of body scanners. Canada has deployed 15 machines so far and officials there are planning to install a further 29, while Russia has been using scanners at airports since 2008[294] and Nigeria installed them in late 2010[295]. The Australian government announced its intention to deploy scanners in late 2011 as has Japan, India, South Africa and Kenya.[296] The European Commission also reports that China (including Hong Kong) and South Korea are interested in the technology.[297] However, the situation in India remains unclear as the outcome of testing in 2006 was a decision by the Central Industrial Security Force (CISF), the organisation responsible for security at Indian airports, to reject the use of body scanners because they were "too revealing and offend passengers, as well as embarrass their security officials"[298].

In addition to airports, body scanners are being deployed in other contexts. For example, L-3 ProVision millimetre wave scanners are deployed in "Israel's new advanced border crossing ...control checkpoints in Iraq's International Zone (Green Zone), facilities in Afghanistan as part of the NATO contingent, [and] a data center in Tokyo. [...] Additionally, the system is currently installed and under evaluation at the District of Colombia's Federal Courthouse, the El Paso County Terry R. Harris Judicial Complex in Colorado Springs, Colorado, and other US government facilities."[299] The systems are also used in correctional facilities in the USA to check for weapons, drugs or other prohibited materials.[300]

Alternative and near future developments

Emerging applications in the field of body scanning include expanding the capabilities of current technologies, as well as expanding the uses to which body scanning can be put. Expanding the capabilities of current technology includes examples such as the newly introduced, potentially covert "Walk-By System 350" and "Stand-Off System 350" developed by Millivision. The walk-by system is designed for use in "mass transportation venues, shopping malls and entryways to public buildings" and involves individuals walking at a normal pace through

[291] JetSetCD, "Updated: What Airports Have Full-Body Scanners Right Now", *Jaunted*, 2 Mar 2010. http://www.jaunted.com/story/2010/3/1/232031/9854/travel/Updated%3A+What+Airports+Have+Full-Body+Scanners+Right+Now
[292] L-3 Communications, "TSA to Test L-3 Millimeter Wave Portals at Phoenix Sky Harbor Airport", 11 Oct 2007. http://www.l-3com.com/news-events/pressrelease.aspx?releaseID=1061924
[293] Privacy International, *Norway - Privacy Profile*, 23 Jan 2011. https://www.privacyinternational.org/article/norway-privacy-profile
[294] European Commission, op. cit., 2010.
[295] Associated Press, op. cit. 2009.
[296] European Commission, op. cit., 2010.
[297] Ibid.
[298] Cavoukian, Ann, *Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy*, Information and Privacy Commissioner Ontario, Canada, March 2009, p. 2.
[299] L-3 Communications, "TSA to Test L-3 Millimeter Wave Portals at Phoenix Sky Harbor Airport", 11 Oct 2007.
[300] airport-technology.com, "Cook County Selects L-3 ProVision™ Whole Body Imaging Solution for Deployment across Large Prison Complex", 10 Feb 09. http://www.airport-technology.com/contractors/security/l-3_security/press22.html

corridors which appear normal but which scan individuals using passive millimetre wave cameras.[301] The stand-off system is designed similarly but individuals walk past normal looking walls and are scanned at a distance of up to 13 feet.[302] Smiths Detection's B-SCAN system can also "detect objects concealed in body cavities or artificial limbs as well as hidden on a person" and can also see through turbans or other head dressings as well as inside shoes.[303] The TSA reports that they are considering the use of mobile passive millimetre wave scanners.[304] For example, DSE International manufacture a "lightweight handheld millimetre wave scanner" that "allows security personnel to scan in real time areas that are difficult to reach without embarrassing passengers or customers... especially those with cultural traditions where physical checks are considered invasive."[305] Finally, Klitou reports that a company called ThruVision has developed a "passive terahertz imaging system [that] is equally capable of revealing both metallic and non-metallic objects hidden under clothing on still or moving persons", that detects concealed objects "without ever displaying physical details of the body".[306] Outside of the security sector, millimetre wave body scanners are also being used in retail for tailoring and other customer measurements, to help customers achieve "custom made clothing" and "a perfect fit".[307]

Other emerging technologies in respect of security checks for contraband material primarily include explosives detectors. Smiths Detection manufactures a product called Sentinel II that can detect minute quantities of explosives or drugs on a person.[308] Klitou also finds that General Electric's product EntryScan can detect trace particles of explosives, and has already been deployed at airports in the US, while Ahura's FirstDefender can "detect explosives or other chemicals in sealed plastic or glass containers".[309] Another programme financed by the US government, Future Attribute Screening Technology (FAST), involves individuals walking through a portal while sensors monitor their vital signs, for example, heart rate, to attempt to identify "malintent".[310] Scientists are also developing biometric systems based on body scans, where the scanning of skeletal features at a distance and subsequent matching on a database would allow authorities to identify individuals of interest without having to approach them.[311]

---

[301] Millivision, "Walk-By System 350: Efficient Threat Detection", 2009. http://www.millivision.com/walk-by-350.html

[302] Millivision, "Stand-Off System 350: Unobtrusive Threat Detection", 2009. http://www.millivision.com/stand-off-350.html

[303] Smiths Detection, "People screening systems", 2011. http://www.smithsdetection.com/millimeter-wave_inspection.php

[304] The TSA Blog, "More on Passive Millimeter Wave Technology", 5 Sept 2008. http://blog.tsa.gov/2008/09/more-on-passive-millimeter-wave.html

[305] DSE International, "EOD305 Handheld Passive Millimeter Wave Scanner", 2011. http://www.dseinternational.com/content/products/Product.aspx?Id=216

[306] Klitou, 2008, p. 319.

[307] Unique Scan, "Custom clothing and apparel", 2011. http://www.uniquescan.com/

[308] Smiths Detection, 2011.

[309] Klitou, 2008, pp. 319-320. However, the New York Civil Liberties Union (NYCLU) are suing the Department of Corrections because prison visitors who test positive, or who refuse the test, are not allowed to enter prison and their photographs are linked to positive scan results and circulated to prison officials to identify those persons during future visits. See ACLU, "NYCLU Sues State Department of Corrections for Information about Controversial Method for Screening Prison Visitors for Drugs", 26 May 2010. http://www.aclu.org/drug-law-reform-prisoners-rights-technology-and-liberty/nyclu-sues-state-department-corrections-info

[310] Weinberger, Sharon, "Airport security: Intent to deceive?", *Nature*, Vol. 465, 26 May 2010, pp. 412-415. http://www.nature.com/news/2010/100526/full/465412a.html

[311] Goodin, Dan, "Skeletal scanner would ID terrorists from 50 meters: And maybe non-terrorists too", *The Register*, 24 Aug 2010. http://www.theregister.co.uk/2010/08/24/skelital_image_scanner/

4.3.3 Stakeholders and drivers driving the development of the technology

A number of companies and other entities are involved in the development and deployment of body scanners in airport environments. The following table (Table 4.1) gives an indication of which companies are heavily involved in developing these systems and their products.

Product	Company	Type	Capabilities	PETs
Smartcheck	American Science and Engineering, Inc.	Backscatter x-ray	Can see through clothing	Privacy image software with a generic human figure is available.
Ait84	Tek84	Backscatter x-ray	Can see through clothing as well as turbans, hijabs, burqas and can scan feet.	No
Castscope	Tek84	Backscatter x-ray	Can see through casts	No
Rapiscan Secure 1000 Single Pose	Rapiscan	Backscatter x-ray	Can see through clothing	No
GEN 2	Brijot	Passive millimetre wave	Can see through clothing and can be deployed remotely at 5-9 feet.	No anatomical details revealed.
eqo	Smiths Detection	Active millimetre wave	Can see through clothing.	Soon to be available software with generic human figure and highlighted areas.
Portal system 350	Millivision	Passive millimetre wave	Can see through clothing.	Automated Threat Detection tool that highlights suspect areas on a blurred or generic human figure.
Walk-by system 350	Millivision	Passive millimetre wave	Can see through clothing. Passive, potentially covert scanning through corridors.	Automated Threat Detection tool that highlights suspect areas on a blurred or generic human figure.
Stand-off system 350	Millivision	Passive millimetre wave	Can see through clothing at a distance of 3-4 meters. Passive, potentially covert scanning along standard corridors.	Automated Threat Detection tool that highlights suspect areas on a blurred or generic human figure.
Handheld passive millimetre wave scanner	Defence and Security Equipment International	Passive millimetre wave	Can see through clothing. Handheld, portable system.	Blurred image.
ProVision	L-3 Communications	Active millimetre wave	Can see through clothing and packaging	Automated Threat Detection software
Rapiscan Secure 1000 Dual pose	Rapiscan	Backscatter X-ray	See through clothing	No

Product	Company	Type	Capabilities	PETs
B-Scan	Smiths Detection	X-ray	Detects objects concealed internally and externally. Can see through shoes.	No
	Tianjin Chongfang Science and Technology Company	Anti-scattering X-ray	Can locate prohibited objects in a fasting-moving mix of crowds.[312]	Automatically deletes images.

Table 4.1: Manufacturers of body scanning systems

In addition, Pacific Northwest National Laboratory (not listed in the table above) developed the first millimetre wave scanner and sold the patent to L-3 Communications. PNNL has strong links with the Department of Homeland Security and has been heavily involved in government contracts for the development of security technologies. Body scanning systems are estimated to cost approximately $130,000 to $170,000 USD, making them a significant investment. [313]

These technologies are deployed by various government, law enforcement and security authorities, primarily airport authorities in various countries. One of the primary users of body scanners is the Transportation Security Administration (TSA) in the USA which is overseen by the Department of Homeland Security. In the UK, systems are procured by the Department for Transport and scanners in Schiphol are managed by the National Counter-Terrorism Co-ordinator, Customs and Schiphol Airport in partnership. In the USA, scanners in jails and other correctional facilities are procured by the Department of Corrections or various state level agencies.

However, other stakeholders are also involved in the discussions around the implementation of body scanners in various contexts. Key civil society organisations (CSOs) such as Privacy International, the ACLU and the Electronic Privacy Information Center (EPIC) have all raised concerns about the use of body scanners. Other organisations such as the Commission Nationale de l'Informatique et des Libertés (CNIL) in France, Bits of Freedom in the Netherlands and Flyersrights.org in the USA have all taken a critical stance on the use of body scanners in airports in particular. Furthermore, it is not only CSOs who have been critical: the national police union in Germany (GdP) has declared itself against the use of body scanners[314]. Various European government agencies and committees have also come out against their use. For example, both the European Economic and Social Committee and the Article 29 Data Protection Working Party (Art. 29 WP) have criticised the current use of body scanners in airports. And finally, a UK member of the European Parliament was credited with calling airport body scanners a "virtual strip search".[315]

[312] Xinhua, "China's new body scanner debuts, promises privacy", 21 Apr 2011. http://news.xinhuanet.com/english2010/china/2011-04/21/c_13840130.htm
[313] Heussner, Ki Mae, "Air Security: Could Technology Have Stopped Christmas Attack?", *ABC News*, 29 Dec. 2009. http://abcnews.go.com/Technology/AheadoftheCurve/air-security-technology-stopped-xmas-attack/story?id=9436877
[314] UPI, op. cit., 2009.
[315] *EDRi-gram*, "The European Parliament says no to airport body scanners", No. 6.21, 5 Nov 2008.

Benefits, gaps and losses

Despite this heavy criticism, many authorities, journalists, academics, industry experts and other stakeholders point out that there are clear beneficiaries of airport body scanners, including most groups of passengers. The European Commission has pointed out that a weakness in aviation security is the inability to detect non-metallic items, and that the quality hand searches varies across airports, as well as being intrusive, time-consuming, labour-intensive and expensive.[316] Klitou agrees, stating that "backscatter body scanners can significantly enhance the security screening process at airports and reduce the adverse effects of 'human factors', by facilitating security screeners to detect any object hidden on a person that metal detectors and sometimes a pat down cannot".[317] Millivision states that "we can no longer rely upon the ubiquitous metal detectors or disruptive security checkpoints to keep us safe... Nor can we enjoy normal social or commercial interactions if we interrupt the free flow of people in airports, office buildings and government installations with intrusive security measures".[318] The Tek84 Engineering Group asserts that their Ait84 product will "increase the speed of security checks while providing convenience and comfort to passengers" because it is capable of screening "the feet, turbans, hijab, burqa and some casts and prosthetics".[319] Additionally, Mironenko notes that body scanners are thought to better protect the travelling public, and they "are supposed to improve passenger flow by performing screening at a very acceptable speed".[320] Indeed many journalists report that passengers prefer scanning to physical pat-down searches, and appreciate not having to remove clothing items to pass through security.[321] Comments by individual passengers in a *BBC News* article support this view: for example, Steven Todd from Glasgow states that "If it meant that as passengers we were more secure and also meant we didn't have to go through the added hassle of undressing then I can't see why people would complain, especially given the authorities assurances that the images are destroyed".[322]

Despite authority and industry claims that scanners offer increased security in terms of detecting concealed weapons, many academics, journalists and other stakeholders argue that significant gaps remain in the ability of machines to offer increased security for passengers. A number of stakeholders have pointed out that the machines cannot detect items hidden inside body cavities or folds of skin, and that some materials can be taped to an individual's abdomen and thus be mistaken for normal anatomy.[323] Mironenko, in particular, notes that manufacturers of the body scanners used at Schiphol Airport admit that their scanners would not have detected the materials concealed by the "underwear bomber" because the substance he

[316] European Commission, 2009, op. cit., p. 2.
[317] Klitou, op. cit., p. 318.
[318] Millivision, "Millivision Technologies Threat Detection Systems", 2009. http://www.millivision.com/
[319] Tek84 Engineering Group, "Body Scanner", 2011. http://www.tek84.com/bodyscanner.html
[320] Mironenko, Olga, "Body scanners versus privacy and data protection", *Computer Law & Security Review*, Vol. 27, No. 3, 2011, p. 2.
[321] See BBC News, "'Naked' scanner in airport trial", 13 Oct 2009. http://news.bbc.co.uk/1/hi/uk/8303983.stm; *Welt Online,* "EU lawmakers criticize 'virtual strip search'", 23 Oct 2008. http://www.welt.de/english-news/article2614271/EU-lawmakers-criticize-virtual-strip-search.html; Rosen, Jeffrey, "Nude Awakening", *The New Republic*, 29 Jan 2010. http://www.tnr.com/article/politics/nude-awakening; Etzioni, Amitai, "Private Security: In defense of the 'virtual strip-search'", *The New Republic*, 9 Oct 2010. http://www.tnr.com/article/politics/78250/private-security-virtual-strip-search
[322] BBC News, op. cit., 13 Oct 2009.
[323] Kravitz, op cit.,2010; Mironenko, 2011, p. 9; Schwartz, John, "Debate Over Full-Body Scans vs. Invasion of Privacy Flares Anew After Incident", *The New York Times*, 29 Dec 2009. http://www.nytimes.com/2009/12/30/us/30privacy.html; Deane, Alexander, "Better Safe?", *IPA Review*, June 2010, p. 21.

carried was not detectable and the detonator was hidden in a body cavity.[324] Alongside Mironenko, Kravitz also notes that, in a TSA pilot, the detection of weapons and other contraband items varied considerably depending on which operator was evaluating the images, and furthermore that "'backscatter' rays can be obscured by body parts and might not readily detect thin items seen 'edge-on'".[325] Furthermore, others have argued that the costs of scanners at major airports will be passed on to flyers[326], that those who value securing and maintaining their privacy will be negatively affected[327], and that scanners will fail to catch "criminals" but will "subject the rest of us to intrusive and virtual strip searches"[328]. Salter notes that the use of body scanners as a secondary screening procedure could enhance the effects of racial profiling.[329] Kessler and Seeley estimate that "full body scanner usage at airports will increase annual highway driving fatalities from as few as 11 additional deaths to as many as 275" because those who are concerned about privacy will drive instead.[330] Finally, Peterson notes that Muslim women in particular will not benefit as religious beliefs about modesty are violated by compulsory body scans and this could affect Muslim women's ability to travel by air.[331] In fact, she states that in the UK, two Muslim women travelling to Pakistan had to forfeit their right to travel as a result of their refusal to undergo a body scan.[332]

4.3.4 Privacy impacts and ethical issues raised by the technology

Despite these serious criticisms, the most significant "loss" discussed in relation to body scanners is the loss of privacy. Privacy concerns were mainly centred around two key issues, the revealing of individuals' naked bodies, including revealing information about medical conditions, and the protection of the personal data that the scans would generate.

In terms of revealing naked bodies, privacy advocates argue that this loss of privacy is disproportionate to any gains in security. Academics, privacy advocates, politicians and journalists have all warned that the images reveal an individual's "naked body", including "the form, shape and size of genitals, buttocks and female breasts".[333] These stakeholders include Bill Scannell, a privacy advocate and technology consultant[334], Barry Steinhardt of the American Civil Liberties Union (ACLU)[335], German newspaper *Welt Online*[336], Micheal Vonn, policy director of the British Columbia Civil Liberties Association[337], Alex Deane, director of Big

[324] Mironenko, op. cit., 2011, p. 9.
[325] Kravitz, op. cit., 2010.
[326] Deane, op. cit., 2010.
[327] Kessler, Mary Elaine, and Brett R. Seeley, "Predicting the Impact of Full Body Scanners on Air Travel and Passenger Safety", Naval Postgraduate School, MBA Professional Report, June 2010.
[328] Rucker, Philip, "US airports say seeing is believing as passengers face body-scan drill", *Sydney Morning Herald, 5 Jan 2010.* http://www.smh.com.au/travel/travel-news/us-airports-say-seeing-is-believing-as-passengers-face-bodyscan-drill-20100104-lq6o.html
[329] Centre for European Policy Research, "Body Scanners", IN:EX Roundtable, 27 Jan 2011. http://www.ceps.eu/content/proceedings-selection-inex-meetings
[330] Kessler and Seeley, op. cit., 2010, p. v.
[331] Peterson, Rohen, "The Emperor's New Scanner: Muslim Women at the Intersection of the First Amendment and Full Body Scanners", *Social Science Research Network*, 6 Mar 2010. http://ssrn.com/abstract=1684246
[332] Ibid.
[333] Klitou, op. cit., 2008, p. 317. See also, Schwartz, op. cit., 2009 and CBC News, "Airport scanners invade privacy: advocate", 5 Jan 2010. http://www.cbc.ca/canada/british-columbia/story/2010/01/05/bc-airport-scanners-civil-liberties-vonn.html,
[334] Klitou op. cit., 2008.
[335] Ibid.
[336] Schwartz, op. cit, 209.
[337] CBC News, op. cit., 2010.

Brother Watch[338], US Representative Jason Chaffetz[339] and British Conservative MEP Philip Bradbourn[340], to name a few. Concerns about the improper viewing of naked images of individuals was given significant weight once it emerged that a security operative at Britain's Heathrow Airport was cautioned by police after "ogling" a female colleague who unwittingly stepped into a body scanner.[341] Finally, the supposed widespread public acceptance of body scanning in favour of pat-down searches was undermined by findings at Orlando International Airport that "at least 25% of passengers refused to submit to the scanning after viewing a sample image".[342] As a result, EPIC report that "[a]ctivism soon sprang up in unexpected places and spread virally; some people created the 'scanners opt-out day', the 'we won't fly' campaign and other initiatives".[343]

Privacy advocates also warn that the images show details of medical conditions that may be embarrassing for individuals. As early as 2002, the ACLU were asserting that "Passengers expect privacy underneath their clothing and should not be required to display highly personal details of their bodies such as evidence of mastectomies, colostomy appliances, penile implants, catheter tubes and the size of their breasts or genitals as a pre-requisite to boarding a plane".[344] In an article by *EDRi-gram*, a British Conservative MEP, Philip Bradbourn, argued that body scans "were a grave violation of the right of privacy and a degrading measure".[345] The issue of "naked images" has also raised questions about child protection laws. EPIC has raised concerns about the capacity for public viewing as well as storage and recall of images of children.[346] Privacy International has called the use of scanners on under-18s, "electronically strip searching children and young people".[347] In the UK, trials of the scanners at Manchester Airport were halted because Action for Rights of Children claimed that the scanners violated the Protection of Children Act of 1978 by creating nude images or pseudo-images of children.[348] The trials were only re-started after under-18s were exempted from scans. However, Mironenko notes that such exemptions could paradoxically introduce a risk that children would be recruited by terrorists.[349] The UK Department for Transportation has said that they believe that body scanners constitute a "proportionate and legitimate interference" in relation to both child protection issues and human rights issues, given the security concerns that body scanners address.[350]

---

[338] Haines, Lester, "Heathrow security man cops perv scanner eyeful", *The Register*, 24 Mar 2010. http://www.theregister.co.uk/2010/03/24/heathrow_body_scanner/
[339] Schwartz, op. cit., 2009.
[340] *EDRI-gram*, op. cit., 2008.
[341] Haines, op. cit., 2010.
[342] Electronic Privacy Information Center (EPIC), "Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding", June 2005. http://epic.org/privacy/surveillance/spotlight/0605/
[343] Centre for European Policy Studies, op. cit., 2011.
[344] ACLU, "The ACLU's view on body scanners", 15 Mar 2002. http://www.aclu.org/technology-and-liberty/body-scanners
[345] *EDRI-gram*, op. cit.,, 2008.
[346] EPIC, op. cit., 2005.
[347] Privacy International, "PI statement on proposed deployments of body scanners in airports", 31 Dec 2009. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-565802&als[theme]=Border%20and%20Travel%20Surveillance
[348] Blake, Heidi, "Full body scanners may break child pornography laws", *The Telegraph*, 5 Jan 2010. http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/6933898/Full-body-scanners-may-break-child-pornography-laws.html See also, Mironenko, 2011.
[349] Mironenko, op. cit., 2011.
[350] Department for Transportation, *Impact Assessment on the use of security scanners at UK airports*, 29 Mar 2001.

The second major privacy concern is focused on the possible storage or transmission of images. Although the TSA claim that none of the scanners used in US airports store, print or transmit images[351], a Freedom of Information Act request by EPIC to the TSA found that all machines come with the capability to store and transmit images, although this capability is apparently disabled when they are deployed to airports.[352] EPIC argue that, despite this disabling, the possibility that it can be re-enabled creates significant privacy risks to individuals[353], and furthermore that the TSA has not had an excellent track record in protecting passenger data.[354] Privacy International is concerned that some employees will experience an "irresistible pull" to store or transmit images if a "celebrity or someone with an unusual... body goes through the system".[355] In fact, in Nigeria, airport security operators have been caught rushing "over to the line in order to catch a glimpse of some of the passengers entering the machine and then immediately returned to view the naked images in order to match the faces of their favorites with the images".[356] In a Florida courthouse that was using millimetre wave technology, "agents retained 35 000 images which were then posted on the Internet, breaching the fundamental rights of thousands of people."[357] The prosecution of those who are found to be in possession of prohibited items may also require that images be retained somewhere in the machine. Although the European Commission report states that the discovery of the prohibited item would form the basis of the prosecution of the individual, this may not be sufficient in the future.[358] Similarly, the TSA have required in their procurement specifications that the machines must also support Ethernet and TCP/IP hook-ups.[359] Although the TSA state that the machines will not be connected to the Internet and, thus, cannot be hacked[360], some have raised the possibility that images could be accessed by persistent hackers with proprietary data[361].

The effects of the use of body scanners on air travellers leads to concerns related to other fundamental rights. According to Privacy International, the use of body scanners amounts to a significant – and for some people humiliating – assault on the essential dignity of passengers that citizens in a free nation should not have to tolerate.[362] The group also cautions that "intrusive technologies" are often introduced with a range of safeguards, but once the technology gains public acceptance, these safeguards are gradually stripped away.[363] As mentioned above, the revealing of naked images could prevent some individuals from using air transpor-

[351] Heussner, op. cit., 2009.
[352] Zetter, Kim, "Airport Scanners Can Store, Transmit Images", *Wired News*, 11 January 2010. http://www.wired.com/threatlevel/2010/01/airport-scanners/
[353] Rucker, op. cit., *2010.*
[354] EPIC, op. cit., 2005.
[355] Privacy International, op. cit., 2009. See also Rosen, op. cit., 2010.
[356] Mironenko, 2011, p. 7.
[357] European Economic and Social Committee, Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM(2010) 311 final, Brussels, 16 Feb 2011, p. 4.
[358] Mironenko, op. cit., 2011.
[359] Mellor, Chris, "US airport body scanners can store and export images", *The Register*, 12 Jan 2010. http://www.theregister.co.uk/2010/01/12/tsa_body_scanners/
[360] Zetter, op. cit., 2010.
[361] Ramachandran, Arjun, "X-ray security: can airport system be hacked?", *Sydney Morning Herald*, 7 Jan 2010. http://www.smh.com.au/technology/technology-news/xray-security-can-airport-system-be-hacked-20100107-lvyq.html
[362] Privacy International, op. cit., 2009.
[363] ACLU, "Backgrounder on Body Scanners and 'Virtual Strip Searches'", 8 Jan 2010. http://www.aclu.org/technology-and-liberty/aclu-backgrounder-body-scanners-and-virtual-strip-searches

tation entirely, including Muslim women and religious Jewish women[364], as well as any others "whose religious beliefs include a perspective on bodily modesty"[365]. This is particularly problematic in countries such as the UK, where individuals forfeit their right to fly if they refuse a scan.[366] Klitou argues that figures related to the use of body scanners in the USA mean that millions of people are subject to "a strip search by electronic means in order to exercise their right to travel".[367] Finally, the ability of individuals to exercise their rights in relation to data protection could become complex and paradoxical. For example, the ACLU analysed the 1,000 complaints they received in one month about TSA screening practices and found that individuals did not complain directly to the TSA because they did not know they could, they thought that it would be useless and/or they were concerned about reprisals such as being put on watch lists by the TSA.[368] Furthermore, Mironenko notes that as part of the European Charter of Fundamental Rights, individuals must have the right to see, correct and remove information that is collected about them.[369]

4.3.5 Extent to which the existing legal framework addresses the privacy impacts

Given the various and significant concerns about privacy and other fundamental rights, those who manufacture, use and deploy body scanners have made use of a number of protections to address these concerns. This includes accepting industry standards, implementing codes of practice, following or suggesting ethical guidance and legislating the use of scanners.

Industry standards

Security screening systems that use x-rays, such as backscatter x-ray scanners, often adhere to or are compatible with the American National Standard N43.17 (ANSI N43.17). This standard provides manufacturers, distributors, installers and users with guidelines on the radiation safety aspects of the x-ray systems.[370] It also "precludes the frivolous use of the security devices where no benefit is to be derived."[371]

Privacy enhancing technologies

The term privacy enhancing technologies (PETs) refers to "coherent systems of information and communication technologies that strengthen the protection of privacy in information systems by preventing the unnecessary or unlawful collection, use and disclosure of personal data, or by offering tools to enhance an individual's control over his/her data".[372] Cavoukian notes that through the use of PETs, gains in security do not have to come at the expense of

[364] Quinn, Ben, "Why Europe doesn't want an invasion of body scanners", *Christian Science Monitor*, 26 Jan 2010. http://www.csmonitor.com/World/Europe/2010/0126/Why-Europe-doesn-t-want-an-invasion-of-body-scanners
[365] CBC News, op. cit., 2010.
[366] Mason, Wyatt, "Scanners Gone Wild", *The New York Times*, 3 Dec 2010. http://www.nytimes.com/2010/12/05/magazine/05FOB-wwln-t.html?ref=technology
[367] Klitou, op. cit., 2008, p. 323.
[368] ACLU, "ACLU Continues To Receive Complaints About New Airport Screening Procedures", 2 Dec 2010. http://www.aclu.org/national-security-technology-and-liberty/aclu-continues-receive-complaints-about-new-airport-screeni
[369] Mironenko, op. cit., 2011.
[370] Health Physics Society, "American National Standard N43.17: Radiation Safety For Personnel Security Screening Systems Using X-rays", 09 July 2010. http://www.hps.org/hpssc/N43_17_2002.html
[371] Ibid.
[372] Cavoukian, op. cit., 2009, p. 1.

privacy, and that technological fixes can enable all parties to benefit from technological advances through incorporating privacy protections into security technologies at the outset.[373]
In relation to body scanners, privacy enhancing technologies can include work to obscure faces or other intimate regions of the body. For example, researchers at Carnegie Mellon's CYLAB have developed software that automatically analyses and then blurs sensitive areas of the body without removing other details.[374] Some manufacturers have installed such protections to ensure that images cannot be inappropriately viewed or misused. L-3's Provision automatically blurs the face and genitals of scanned individuals.[375] AS&E provides remote monitoring stations and removes the capability of images to be stored or transmitted.[376] A range of companies now offer some sort of software that automatically detects anomalies and removes the need for an operator to examine images. Millivision's tool superimposes millimetre detection results onto a CCTV image of the person, resulting in a highlighted box over the area suspected to include a threat.[377] Smiths Detection and AS&E machines also produce an image with an outline of the human body rather than anatomical features.[378] Schiphol has been a leader in utilising these sorts of privacy enhancement tools, and was the first location in the world where the automated images were utilised.[379] Schiphol also notes that this enables children to use the scanners without engendering child protection issues.[380] However, it is important to note that "naked" images are captured by the machines and exist somewhere in their hardware.

Interestingly, another market for privacy enhancing technologies is being developed in response to body scanners. Wikipedia notes that one company is selling x-ray absorbing underwear to protect individual's privacy when being scanned by an x-ray backscatter machine, while another product called Flying Pasties is "designed to obscure the most private parts of the human body when entering full body airport scanners".[381]

Codes of practice

In addition to PETs, for which the manufacturer is often responsible, those who procure and use body scanners often set down codes of practice to address privacy concerns. The Department for Transport in the UK has made portions of their code of practice available to the public.[382] Furthermore, both the Department of Homeland Security in the US and Canadian Air Transport Security Authority (CATSA) have undertaken privacy impact assessments (PIAs) for the integration of body scanners into national airports. The DHS PIA includes information about their code of practice, while some of the codes of practice for the trial of body scanners at Canadian airports are also outlined in the Canadian Privacy Commissioner's annual 08-09

[373] Ibid.
[374] Ibid.
[375] *airport-technology.com*, "TSA Approves L-3's ProVision Millimeter Wave Checkpoint Screening System", 4 Dec 09. http://www.airport-technology.com/contractors/security/l-3_security/press35.html
[376] AS&E, "Privacy-Enhanced Smartcheck", 2011.
http://www.as-e.com/products_solutions/smartcheck_privacy.asp
[377] Millivision, "Portal System 350: Turnkey Threat Detection", 2009. http://www.millivision.com/portal-350.html
[378] Cendrowicz, Leo, "Can Airport Body Scanners Stop Terrorist Attacks?", *TIME Magazine*, Jan. 05, 2010. http://www.time.com/time/world/article/0,8599,1951529,00.html#ixzz1IBr9lbM3 and AS&E, 2011.
[379] Schiphol Airport Security, *Security Scan Brochure*.
http://www.schiphol.nl/Travellers/AtSchiphol/CheckinControl/SecurityChecksUponDeparture/SecurityScan.htm
[380] Ibid.
[381] Wikipedia.org, "Full body scanner", 2011. http://en.wikipedia.org/wiki/Full_body_scanner
[382] See Department for Transport, *Interim Code of Practice*, 2010 and Department of Homeland Security, 2008.

report.[383] These outline the various measures these organisations have undertaken to ensure that passenger privacy is protected during the use of body scanners. These codes of practice share certain features, where for example, all three state that the security officer viewing the body scan image must be physically separate from the person whose image they are viewing. The DfT and CATSA state that the person conducting a physical search should not be able to view the image on the screen, and the Dft further state that the person selected for screening may request a screen reader of the same sex.[384] The TSA, DfT and CATSA have also declared that the image of the passenger must be destroyed once they have moved away from the scanner and that the image cannot be stored, transmitted or retrieved. However, the TSA state that images will be transferred between the machine and the viewer (although they are encrypted)[385] and the DfT state that in "exceptional circumstances", an additional security officer may be required to view the image[386]. Finally, the TSA, DfT and CATSA[387] have recognised the importance of informing passengers about the body scanning technology. The DfT state that "an effective communication strategy should be developed to inform people of the security requirements where body scanners are deployed... Information should be adequate, clear and provided ideally before ticket purchase. In any event it must be provided prior to entering the passenger screening area. Information should also be readily available in a number of languages appropriate for the profile of passengers using the airport."[388] While the TSA have decided that "Informational brochures regarding the program will be made available at each WBI site that will show a WBI image that the technology will create"[389] which will enable passengers to decide between a full body scan and a physical pat down search.

The DfT does differ from other national authorities on key points. One of the major differences is that individuals selected for scanning in American, Dutch and Canadian airports have the option to undergo a pat-down search, while those travelling in Britain must go through the scanner or forfeit their right to travel.[390] Alongside Schiphol Airport, the DfT is also considering using automated threat detection software to enable images to be analysed by a computer rather than a security official.[391] The TSA also states that operators are prohibited from bringing cameras, phones or other photographic equipment into the image viewing area, while the DfT makes no mention of this requirement. The DfT does, however, require that airport operators provide evidence that individuals are not being selected on the basis of personal characteristics, and airports must give persons selected for screening an opportunity to provide personal information, such as gender, age, race or ethnic origin.[392] Finally, the TSA also blurs the faces of individuals selected for screening so that they are unidentifiable to those reviewing the images.

---

[383] Office of the Privacy Commissioner of Canada, Annual Report to Parliament 2008-2009, Report on the Privacy Act. http://www.priv.gc.ca/information/ar/200809/200809_pa_e.cfm.
[384] Department for Transport, *Interim Code of Practice*, 2010.
[385] Department of Homeland Security, 2008, pp. 8-9.
[386] Department for Transport, *Interim Code of Practice*, 2010.
[387] OPC of Canada, "Letter in response to the Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA) in anticipation of the deployment of millimetre wave (MMW) screening technology at selected Canadian airports", 29 Oct 2009. http://www.priv.gc.ca/pia-efvp/let_20100108_e.cfm
[388] Department for Transport, *Interim Code of Practice*, 2010, p. 5.
[389] Department of Homeland Security, 2008, p. 6.
[390] Department for Transport, *Interim Code of Practice*, 2010, p. 5, Schiphol Airport Security, *Security Scan Brochure* and Office of the Privacy Commissioner of Canada, 2009.
[391] Department for Transport, *Interim Code of Practice*, 2010 and Schiphol Airport Security, *Security Scan Brochure*.
[392] Department for Transport, *Interim Code of Practice*, 2010

Despite many of these stated safeguards, Klitou notes that self-regulations such as codes of practice are not binding and could change at the discretion of the body using those regulations.[393]

European law

The issue of body scanners has raised a number of serious potential conflicts with existing European law. Mackey notes that European human rights law includes a respect for the dignity of the individual that prohibits treating people as objects.[394] However, he quotes Murphy and Wilds in contending that:

> utilization of X-ray search devices allows unreasonable, subjective searches of an innocent traveler when little or no evidence of criminality is present. The backscatter device effectively reduces the traveler's body to the same legal status as a piece of luggage on a conveyor belt.[395]

The Transportation Commission also notes that the European Commission has an obligation to "protect persons and goods" within the EU from "acts of unlawful interference with civil aircraft" including hijack or sabotage of aircraft.[396] As a result, the issue of the use of body scanners has been considered by the European Commission and European Parliament since 2008, when a Commission plan to introduce body scanners across European airports was rejected by the Parliament until further information could be provided about the impacts scanners could have on the rights of citizens.[397] In its Resolution of 23 October 2008, the Parliament expresses concerns that body scanners will have a "serious impact on the right to privacy, the right to data protection and the right to personal dignity".[398] The Parliament also notes that the Commission has not presented enough justification for the use of scanners and that there is no regulatory procedures or procedures for screening discussed in the proposal. The Parliament requested that the European Data Protection Supervisor, the Article 29 WP and the Fundamental Rights Agency deliver an opinion on the use of body scanners in order to assess their impact on the principle of proportionality and citizens fundamental rights.[399] The document also requests that the Commission carry out an impact assessment relating to fundamental rights, a scientific and medical assessment of the health risks of the technologies as well as a cost-benefit analysis of the technologies.[400] However, according to a Commission Communication, while individuals currently do not have the right to opt in or out of security measures at EU airports, if European-wide legal regulations on the use of scanners were implemented, special protection for vulnerable individuals such as pregnant women or children would be considered.[401]

---

[393] Klitou, 2008.
[394] Mackey, David A., "The 'X-Rated X-Ray': Reconciling Fairness, Privacy, and Security", *Criminal Justice Studies*, Vol. 20, No. 2, June 2007, pp. 149–159.
[395] Murphy and Wilds, 2001 quoted in Mackey, ibid., p. 156, .
[396] Transport Commission, Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, 19 Feb 2009. http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm
[397] UPI, op. cit., 2009.
[398] European Parliament, Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, RSP/2008/2651. http://www.europarl.europa.eu/oeil/FindByProcnum.do?lang=en&procnum=RSP/2008/2651
[399] European Parliament, 2008.
[400] Ibid.
[401] European Commission, Commission communication on the use of security scanners at European airports — questions and answers, MEMO/10/261, Brussels, 15 June 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/261&format=HTML&aged=0&language=EN&guiLanguage=e

Although the use of body scanners is not regulated at the European level, individual Member States have two options in relation to the introduction of body scanners. They can either exercise "their right to apply security measures that are more stringent than existing EU requirements", or they can conduct a trial of the scanners for a period of up to 30 months.[402] The EC vice president, Antonio Tajani, has stated that a European solution to the use of body scanners was preferable to "individual member states deciding on their own".[403] Yet, there is no consensus among Member States on the use of body scanners in airports. While the UK and the Netherlands have been enthusiastic about adopting them, Spain, Germany, France and Belgium have expressed reservations.[404] A number of countries have exercised their right to conduct trials of up to 30 months. The French government has recently approached its National Assembly for permission, and German authorities are installing the scanners for a six-month trial at Hamburg's Fuhlsbuettel Airport, while Italy, after undertaking a similar trial, has decided to drop the use of scanners.[405] Finland has also decided to discontinue the use of scanners after an 18-month trial because of privacy concerns and the European Parliament's decision not to recognise body scanners as approved security measures.[406]

National laws

Even within nations, legislation or other legal issues can impact the implementation of scanners. In the UK, the laws relevant to the use of body scanners include anti-discrimination laws, child protection laws and rights to privacy. In 2010, *The Telegraph* reported that the Equality and Human Rights Commission expressed concerns that scanners being used in the UK were "breaking discrimination laws as well as breaching passengers' rights to privacy".[407] The Equality and Human Rights Commission is considering mounting a high court challenge regarding the use of scanners.[408] Furthermore, passengers in Britain do not have the right to choose an alternative method of security control, as they do in the US. Mironenko notes that this could contravene Article 13 of the Universal Declaration on Human Rights, which states that "everyone has the right to leave any country, including his or her own, and to return to his or her country."[409]

In France, a new bill on internal security was necessary in order to introduce body scanners, and then only for a three-year period. The French National Assembly asked the French data protection authority CNIL to review the bill and make recommendations as to their deployment. CNIL has recommended that in relation to body scanners, in addition to removing the storage capability for images, the bill should introduce measures to set out who had authorised access to images and how these images could be accessed by authorised individuals.[410]
In the USA, the use of body scanners is covered by the Fourth Amendment, which "gives individuals freedom from any unreasonable search and seizure conducted by the US Gov-

[402] Mironenko , 2011, p. 4.
[403] "EU considers full body screening in airports", 2010.
[404] "EU considers full body screening in airports", 2010.
[405] Mironenko, 2011.
[406] Mironenko, op. cit., 2011.
[407] *The Telegraph*, "Airport body scanners 'may be unlawful'", 15 Feb 2010.
http://www.telegraph.co.uk/travel/travelnews/7242087/Airport-body-scanners-may-be-unlawful.html
[408] Travis, Alan, "Anti-terror body scanners may be illegal, ministers warned", *The Guardian*, 16 Feb 2010.
http://www.guardian.co.uk/uk/2010/feb/16/uksecurity-terrorism
[409] Mironenko, op. cit., 2011, p. 5.
[410] Ernst and Young, "France", *Update IP/ICT Legal Practice*, No. 5, Oct 2010, p. 3.

ernment".[411] Klitou explains that while the original law only protected individual property, the US Supreme Court later extended their interpretation of the Fourth Amendment to include a consideration of searches of the person, particularly where a person has a reasonable expectation of privacy. However, individuals have less of an expectation of privacy in certain places, for example, at borders, or when engaging in certain activities, such as air travel. As such, searches at airports are considered reasonable searches under the Fourth Amendment, which includes the use of body scanners.[412] However, Klitou notes that while border searches are considered reasonable, "strip searches" at borders are not reasonable without probable cause, and those exercising their freedom to travel do not automatically give up their privacy rights to do so.[413] However, US law, as it currently stands, does not recognise the use of body scanners as a strip search and, consequently, "TSA airport screeners or Transportation Security Officers (TSOs) are at present immune from legal action for any inappropriate use of backscatter body scanners".[414] Klitou concludes that one danger of this lack of clarity is that the use of body scanners could be expanded to other locations such as sports arenas, mass transport or even shopping malls.[415]

The issue is currently being debated within various forums in relation to US policy. For example, in June 2009, the US House of Representatives passed a bill that would limit the use of whole body imaging to secondary screening purposes.[416] In January 2010, the ACLU presented testimony to three Senate committees discussing counter-terrorism and airline security, the Senate Judiciary Committee, the Homeland Security and Government Affairs Committee and the Commerce, Science and Transportation Committee.[417] In order to better understand the use of body scanners in US airports, EPIC has made a number of Freedom of Information requests to the DHS as well as sued the DHS over its failure to comply fully with those requests. Finally, in February 2011, a bill was introduced in the Senate to require the TSA to install automatic threat detection software on body scanners by January 2012 to reduce threats to passenger privacy. The TSA has announced it will begin testing such software.[418]

4.3.6 Need for new legislation, codes of conduct etc. to deal with privacy impacts not covered by the existing framework and how to deal with ethical issues

The future regulation of the use of body scanners should take into account ethical consideration, provide for privacy enhancing technologies, and include a rigorous code of practice.

Ethics

Some of the principal ethical issues discussed in relation to body scanners relate to dignity (respect for personal modesty) and the principles of informed consent and voluntary submission. For example, Mordini notes that acts that concern the body are invested with cultural

[411] Klitou, op. cit., 2008, p. 320.
[412] Mackey, op. cit., 2007.
[413] Klitou, op. cit., 2008.
[414] Klitou, op. cit., 2008, p. 322.
[415] Ibid.
[416] EPIC, "EPIC v. Department of Homeland Security - Body Scanners", 25 March 2011. http://epic.org/privacy/airtravel/backscatter/epic_v_dhs.html
[417] ACLU, "ACLU Submits Statement On Aviation Security To Key Senate Committees", Jan 20 2010. http://www.aclu.org/national-security-racial-justice-technology-and-liberty/aclu-submits-statement-aviation-security-key
[418] EPIC, op. cit., 2011.

values, and as such ethical assessments of particular technologies should respect non-western cultures. Furthermore,

> No one should ever be obliged to undergo any security measure that he feels humiliating and degrading. In particular no one should be offered the option to accept such a measure in exchange for a benefit. This would make it still more humiliating.[419]

Mackey reviews the ethical technology application standards introduced by Gary Marx and relates these specifically to the use of body scanners. He states that body scanners should only be used in the event of "the absence of physical or psychological harm, awareness of the procedures, consent to the procedures, the golden rule, proportionality of the intrusion given the objectives, consequences of inaction, adequate data stewardship, and [knowing] who benefits from the intervention".[420] As above, informed consent provides a key criterion for establishing ethical deployment of technologies, and he explains that informed consent would also enable passengers to avoid setting off the detectors if they had information about how they worked. Mackey also argues that the potential for unequal application of the technology exists when those with specific resources are able to avoid the technology, for example, by chartering private flights, or if the technology is used disproportionately in some areas, for example, gun crime hotspots.[421]

Privacy enhancing technologies and other industry standards

Acceptance of body scanners might be improved by use of PETs, or other manufacturing standards which address privacy concerns. Cavoukian has stated that the only way to give adequate attention to the privacy invasive potential of whole body imaging scanners is to address these concerns in the design phase of the technology, as well as its deployment and use.[422] The Art. 29 Working Party also notes that an EU-wide technical standard would support a "privacy and data protection friendly deployment of body scanners".[423] Some researchers, policy analysts, public authorities and technical experts advocate the use of automated imaging technology or privacy algorithms that blur or block the face or other personal areas, or use generic human figures and/or highlighted boxes to indicate areas of potential concern.[424] Despite these possibilities, Cavoukian expresses disappointment that there has been very little discussion of such privacy filters in the implementation of body scanners.[425] Another way to respect privacy involves disabling the machines' storage, copying or transmission capabilities. Such controls are supported by Klitou[426], the European Commission[427], the

[419] Ibid., p. 5.
[420] Mackey, op. cit., 2007, p. 154.
[421] Ibid., p. 155.
[422] Cavoukian, op. cit., 2009.
[423] Article 29 Data Protection Working Party, *Response to Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection*, 11 May 2009, p. 14.
[424] Mackey, op. cit., 2007; Klitou, op. cit., 2008; Cavoukian, op. cit., 2009; Art. 29 Working Party, op. cit., 2009; Mordini, Emilio, *Whole Body Imaging at airport checkpoints: the ethical and political context*, HIDE&RISE policy report, February 2010 (updated March 2011). www.riseproject.eu; Hrejsa, Allen F., and Morris L. Bank, "The use of low dose x-ray scanners for passenger screening at public transportation terminals should require documentation of the 'informed consent' of passengers", *Medical Physics*, Vol. 32, No. 3, March 2005, pp. 651–653; European Commission, op. cit., 2010.
[425] Cavoukian, op. cit., 2009. However, Klitou points out that supporters of body scanners argue that such PETs would conceal weapons hidden near the genitals.
[426] Klitou, op. cit., 2008.
[427] European Commission, op. cit., 2010.

Art. 29 Working Party[428] and Mordini[429]. However, Klitou notes that the machines may be able to store images under "exceptional circumstances, for example when the images are necessary for the prosecution of an individual"[430], and Mordini point out that there should be safeguards to ensure that PETs cannot be "switched off".[431]

Other industry bodies attempt to address safety concerns. For example, the Inter-Agency Committee on Radiation Safety, which includes the European Commission, International Atomic Energy Agency, Nuclear Energy Agency and the World Health Organization have stated that air passengers should be made aware of the health risks of airport body screenings, that governments must explain any decision to expose the public to higher levels of cancer-causing radiation and that pregnant women and children should not be subject to scanning.[432]

Legislation

Although PETs or other manufacturing controls offer possibilities for the protection of privacy while increasing security, Klitou cautions that a combination of law and technology is required to provide adequate privacy protections.[433] A range of legislative requirements has been suggested for the emerging regulation of the use of body scanners in airports, many of which have overlapping features.

Firstly, the European Commission has argued that even manufacturing standards and technical specifications would benefit from being legally set in order to ensure the protection of citizens.[434] The French National Assembly has proposed that legislation include the stipulation that body scanners have their image storage functions disabled.[435] Legislation could also make existing or future-oriented codes of practice legally binding to ensure that safeguards are not rescinded once technologies become more widely accepted. Legislation could stipulate that security officers who view images should be separated from the individual whose image they are viewing, cameras and other recording devices could be prohibited and same-sex image viewers could be mandated.[436] Klitou also suggests that laws should criminalise the unlawful storage or public disclosure of body scan images, restrict the use of scanners on pregnant women and children and employ software cloaking.[437] Forward-looking legislation already proposed involves the criminalisation of the misuse of full body images.[438]

There is also a need to ensure that the collection of data from body scanners accords with privacy laws.[439] Abeyatne has noted that since the data collected by body scanners may be subject to trans-border storage, the international community should consider uniform privacy

[428] Article 29 Data Protection Working Party, op. cit., 2009.
[429] Mordini, op. cit., 2010.
[430] Klitou, op. cit., 2008.
[431] Mordini, op. cit., 2010.
[432] Deane, op. cit., 2010, p. 22.
[433] Klitou, op. cit., 2008, pp. 316–325.
[434] European Commission, op. cit., 2010.
[435] Fay Joe, "EU bottoms up committee slates body scanners: Expensive, flaky, not fit for purpose ...", *The Register*, 17 Feb 2011. http://www.theregister.co.uk/2011/02/17/scanner_opinion/
[436] Klitou, op. cit., 2008.
[437] Ibid.
[438] The Associated Press, "NY Sen. Seeks Bill to Deter Body Scan Image Misuse", *The New York Times*, 5 Dec 2010. http://www.nytimes.com/aponline/2010/12/05/us/AP-US-Airport-Security.html?hp
[439] European Commission, op. cit., 2010.

laws and/or author international standards and recommended practices.[440] In accordance with current laws, the Art. 29 Working Party notes that passengers should be given information about what data are processed, what processing is taking place, who is processing the data, what the consequences are for setting off a scanner, who can and cannot use the scanner and where to go for more detailed information.[441] Passengers should also have specific information about effective legal remedies to protect passengers from the misuse of body scanners.[442] New legislation of frameworks, attributes, capabilities, characteristics and qualities of body scanning systems should enable certification of systems and subsequently allow users and citizens to verify if systems are trustworthy.[443] Furthermore, the operating procedures of such systems should be made public.[444]

Finally, concerns about the voluntary nature of body scans have been the focus of recommendations for legislation. The European Economic and Social Committee and Cavoukian have argued that passengers should be allowed to opt out of body scans and that this should not affect their right to fly or cause passengers to suffer any additional burdens or delays by opting for an alternative.[445] However, the Art. 29 Working Party highlights some inconsistencies in the Commission's logic in relation to the voluntary nature of body scanners. They note that scanners would have to be mandatory if existing measures were judged to be insufficient, thus making scanners necessary and proportionate. However, if existing measures offer a viable alternative to body scanners, then the justification for body scanners is unsound.[446]

Codes of practice and independent oversight

Future-oriented mechanisms for regulating body scanners also focus on the role of codes of practice and independent oversight. The Art. 29 Working Party favours the use of "impact assessments" such as those carried out by the DHS in relation to the TSA use of body scanners. The Working Party argues that the assessments should be conducted by independent bodies and their conclusions should be widely displayed.[447] Klitou suggests that, in the USA, compliance with rules should be monitored by independent screening supervisors at each airport rather than personnel of the TSA, and that these independent supervisors should also have the power to dismiss screeners.[448] Supervisors should be directed by an oversight committee in conjunction with the TSA's Office of Civil Rights and Liberties and the Privacy and Civil Liberties Oversight Board, and passengers should have the capacity to bring a claim against the government for the misuse of scanners.[449] The European Economic and Social Committee (EESC) concurs, stating that the Commission should develop protocols to ensure that they respond sufficiently to concerns about fundamental rights.[450]

---

[440] Abeyratne, Ruwantissa, "Full body scanners at airports—the balance between privacy and state responsibility", *Journal of Transportation Security*, Vol. 3, 2010, pp. 73–85.
[441] Article 29 Data Protection Working Party, op. cit., 2009.
[442] European Economic and Social Committee, Opinion on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports COM(2010) 311 final, Brussels, 16 Feb 2011.
[443] Mordini, op. cit., 2010.
[444] Ibid.
[445] European Economic and Social Committee, op. cit., 2011 and Cavoukian, op. cit., 2009.
[446] Art. 29 Working Party, op. cit., 2009.
[447] Art. 29 Working Party, 2009, p. 13.
[448] Klitou, op. cit., 2008.
[449] Ibid.
[450] Ibid.
[450] European Economic and Social Committee, op. cit., 2011.

Mordini also suggests that emerging technologies should be evaluated as soon as practically possible; these evaluations should be completed regularly and new regulations, where necessary, should be implemented quickly.[451]
For its part, the European Commission recommends the following procedures:

- The officer analysing the image ("the reviewer") should work remotely without any possibility of seeing the person whose image is being analysed.
- The reviewer should have no possibility of linking the analysed image to any real person, by applying remote reviewing together with the use of equipment without a storage facility.
- Detailed reviewing of images should be undertaken by a person of the same gender.
- Appropriate methods of automated communication should ensure that the exchange between the reviewer and the screener at the checkpoint is limited to the information necessary to satisfactorily search the person.
- More thorough hand searches should take place in cabins or in specially designated separate rooms.[452]

Cavoukian concurs but adds that there must be "a complete prohibition against any retention or transmission of the images in any format" and that personnel should be banned from bringing photographic devices into the viewing area and connecting storage or communication devices to the machine.[453]

The EESC also raises concerns about health protection for staff and passengers. They state that appropriately qualified, well-paid staff should be the only ones to operate the equipment and that well-qualified staff would reduce the frequency of body scans in the first place.[454] Additionally, the vulnerability of passengers such as pregnant women, children or people with disabilities should be recognised.[455]

Other options

Finally, others have concluded that the use of body scanners potentially takes away from more important technological or procedural considerations. The European Economic and Social Committee believes that the fast-developing nature of the market in security technologies means that the EC should wait for more advanced, less intrusive technologies to be developed that would provide more substantial airport security.[456] The European Commission itself recognises that current security checkpoints are "overburdened" with new methodologies and technologies, that a more holistic approach is required in the future which combines technology with intelligence sharing and human factor analysis.[457] Others, including the EESC, agree that a focus on technology "downplays the importance of enhanced intelligence sharing"[458], while a former head of security for Israeli airline El Al states that "The best security is not technology, the best security is a qualified and well-trained human being."[459]

[451] Mordini, op. cit., 2010.
[452] European Economic and Social Committee, op. cit., 2011, p. 11-12.
[453] Cavoukian, op. cit., 2009.
[454] European Economic and Social Committee, op. cit., 2011.
[455] Ibid.
[456] Ibid., p. 4.
[457] European Commission, op. cit., 2010.
[458] Fay, op. cit., 2011.
[459] Heussner, op. cit., 29 Dec 2009.

4.3.7 Discussion

The combination of current regulation in certain states and recommendations for future oriented regulation indicates key criteria for a comprehensive privacy protection strategy that could protect passengers from physical danger and privacy intrusions. These criteria include ethical considerations such as a respect for modesty and proportional deployment so that particular nationalities, classes and social groups are all subject to the same technological processes. Privacy enhancing technologies, such as automated imaging software, should be made mandatory to protect vulnerable people from undue exposure. Furthermore, industry standards could also disable storage or transmission capabilities on deployed systems. States or regions should also legislate codes of practice and make certain facets of the codes legally binding. These could include provisions for same sex screeners and separate viewing stations for men and women, sanctions for the misuse of images, statutes which ensure that passengers are fully informed of the way that their data is used, a prohibition on bringing photographic equipment into scanning or viewing areas, and finally a legal reassurance that body scans are voluntary with a provision for alternate screening procedures. Finally, oversight committees must ensure that those who deploy body scanning systems undertake regular impact assessments of systems to ensure that passenger privacy is protected alongside changes in procedure or technology.

4.4 UNMANNED AIRCRAFT SYSTEMS, SURVEILLANCE, SAFETY AND PRIVACY

4.4.1 Introduction

Unmanned aerial vehicles (UAVs) can generally be defined as a "device used or intended to be used for flight in the air that has no onboard pilot".[460] These devices are sometimes referred to as drones, which are programmed for autonomous flight and remotely piloted vehicles (RPVs) which are flown remotely by a ground controlled operator.[461] Current generations of UAVs "can be as small as an insect or as large as a charter flight".[462] They can be launched from a road or a small vehicle, but are often large enough to accommodate cameras, sensors or other information gathering equipment.[463] Recently, discussions of UAVs have shifted to refer to unmanned vehicles as unmanned aircraft systems (UASs) to reflect "the fact that in addition to the unmanned aircraft, a complete UAS includes multiple pieces of ancillary equipment, such as vehicle control equipment, communications systems, and potentially even launch and recovery platforms".[464] Industry and regulators have now begun to adopt UAS rather than UAV to refer to unmanned aircraft because it captures all of the different elements of deploying these aircraft.[465] According to McBride, the versatility of these "sys-

[460] Quoted from Aviation Safety Unmanned Aircraft Programme Office, 2008, in McBride, Paul, "Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations", *Journal of Air Law and Commerce*, Vol. 74, 2009, p. 628.
[461] Bolkcom, Christopher, *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance*, Congressional Research Service Report for Congress, 28 June 2004.
[462] Eick, Volker, *The Droning of the Drones: The increasingly advanced technology of surveillance and control*, Statewatch Analysis, No. 106, 2009, p. 1. http://www.statewatch.org/analyses/no-106-the-droning-of-drones.pdf
[463] McCormack, Edward D., *The Use of Small Unmanned Aircraft by the Washington State Department of Transportation*, Washington State Transportation Center, June 2008.
[464] McBride, 2009, p. 629. See also Directorate of Airspace Policy, *CAP 722: Unmanned Aircraft System Operations in UK Airspace – Guidance*, Civil Aviation Authority, 6 Apr 2010.
[465] Unmanned Aerial Vehicle Systems Association, "UAV or UAS?", 2011. http://www.uavs.org/index.php?page=what_is

tems" is one of the strongest drivers in the rapid development of these technologies, where "the identification of new potential uses leads to the adaptation of the systems".[466] The Surveillance Studies Network, in its testimony to the UK House of Lords, asserts that UAVs represent one of the technological forms that characterise "new surveillance".[467]

History of UAVs

Despite recent growth in the UAV/UAS market, UAVs have a relatively long history. The first unmanned aircraft was a torpedo developed in 1915 for the US Navy, which was designed to fly to a specific location and drive into its target.[468] In the Second World War they were used as radio-controlled targets and for reconnaissance missions.[469] From the 1960s to the 1980s, the US and Israeli forces undertook significant research into UAVs.[470] In the 1990s, the Defense Advanced Research Projects Agency (DARPA) and NASA began research into further uses of UAVs, and a number of well-known UAVs such as the Helios, Proteus, Altus Pathfinder and Predator (which was first used by the USA in the Gulf War) resulted from this effort.[471] Wilson asserts that drones were so effective in the Gulf War that "Iraqi troops began to associate the sound of the little aircraft's two-cycle engine with an imminent devastating bombardment", which he says led to "the first instance of human soldiers surrendering to a robot".[472] Growth in this area has recently increased exponentially, particularly because of developments in lightweight construction materials, microelectronics, signal processing equipment and GPS navigation.[473] More than 50 nations currently use drones for military reconnaissance, intelligence-gathering and targeting[474] and as of 2003 at least three dozen nations had active UAV development or application programmes.[475]

However, the civil market for UASs is the largest area of predicted sector growth in the next few years. For example, the UK Civil Aviation Authority has stated that a number of model aircraft have been flying successfully for years "performing aerial work tasks, effectively operating as UAVs".[476] Furthermore, a worldwide survey of existing UASs in 2004 found that 79 per cent are aimed at civil research or dual-purpose operations and that this is likely to

[466] McBride, op. cit., 2009, p. 629.
[467] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State, Vol. 2*, HL Paper 18, Second Report, Session 2008-09, House of Lords, London, 6 Feb 09.
[468] Dunlap, Travis, "Comment: We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search", *South Texas Law Review*, Vol. 51, No. 1, Fall 2009, pp. 173- 204.
[469] *The Economist*, "Unmanned aircraft: The fly's a spy", 1 Nov 2007.
http://www.economist.com/displaystory.cfm?story_id=10059596
[470] Srinivasan, Sumanm, Haniph Latchman, John Shea, Tan Wong and Janice McNair, "Airborne Traffic Surveillance Systems: Video Surveillance of Highway Traffic", *Proceedings of the ACM 2nd international workshop on Video surveillance & sensor networks*, 2004, pp. 131–135.
[471] Nonami, Kenzo, "Prospect and Recent Research and Development for Civil Use Autonomous Unmanned Aircraft as UAV and MAV", *Journal of Systems Design and Dynamics*, Vol. 1, No. 2, 2007, pp. 120-128.
[472] Wilson, J.R., "UAVs: A Worldwide Roundup", *Aerospace America*, June 2003.
https://www.aiaa.org/aerospace/Article.cfm?issuetocid=365&ArchiveIssueID=39
[473] *The Economist*, "Unmanned aircraft: The fly's a spy", 1 Nov 2007.
http://www.economist.com/displaystory.cfm?story_id=10059596
[474] *Strategic Comments*, "The drones of war", Vol. 15, No. 4, 2009, pp. 1-2.
[475] Wilson, op. cit., 2003.
[476] Haddon, D.R., and C.J. Whittaker, *UK-CAA Policy for Light UAV Systems*, UK Civil Aviation Authority, 28 May 2004, p. 2.

continue.[477] This emerging civil market includes potential applications such as emergency services, public security and commercial services.[478]

Due to the significant growth in this industry, the capabilities and uses of UASs vary significantly, especially in relation to newly emerging civil applications. Furthermore, these new civil applications are a significant source of growth for the industry, and have been driven by particular categories of stakeholders, although primarily industry. While some groups such as law enforcement, industry and public authorities certainly do benefit from relatively inexpensive deployments of UASs, their use raises some ethical and privacy concerns and requires a range of regulatory mechanisms to address these concerns. Currently, regulations heavily restrict the civil use of UASs, and although some stakeholders are researching ways to remove these barriers, a small number of other stakeholders are suggesting privacy safeguards to protect citizens from UAS surveillance.

This chapter examines the capabilities of UASs and discusses various civil deployments of unmanned aircraft systems in Europe, the USA and other countries. It examines which stakeholders are involved in the development of the UAS industry and who would benefit from further civil deployment of UASs. It explores privacy and other concerns around UAS deployment and looks at current regulatory mechanisms for the use of UASs in various national air spaces. It ends by considering how future-oriented regulations might simultaneously address privacy and other concerns.

4.4.2 Current status of the technology and expected progress in the near future

Capabilities

UAS have a range of capabilities making them useful not only for military applications, but also the bourgeoning field of civil applications. Specifically, UAS have a "niche" in performing the three Ds: dull, dirty and dangerous work, thereby protecting human pilots from fatigue and various environmental hazards. Brecher notes the following general capabilities for unmanned aircraft systems as opposed to manned systems:

- They can be deployed on demand.
- They have flexibility in tasking: e.g., surveillance, disasters, etc.
- They have plug and play capabilities for their payloads, making tailored systems possible.
- They can support high-resolution imagery or sensors.
- They can cover remote areas.[479]

Given all of these capabilities, UAS can be more suited to certain tasks than manned aircraft. Ollero et al. also note that UASs are heterogeneous and can support the high manoeuvrability and hovering capabilities of helicopters as well as the global views and communications relay

[477] Ibid.
[478] FH Joanneum University of Applied Sciences, "Unmanned Aircraft Systems - Towards Civil Applications", Graz, Austria, 10 Nov 2009. http://www.fh-joanneum.at/aw/home/Studienangebot_Uebersicht/fachbereich_information_design_technologien/lav/news_events_ordner_lav/Archiv/~btch/lav_news_091110/?lan=de
[479] Brecher, Aviva, "Roadmap to near-term deployment of unmanned aerial vehicles (UAV) for transportation applications charge to participants", *UAV 2003: Roadmap for Deploying UAVs in Transportation Specialist Workshop*, 2 Dec 2003, Santa Barbara, California.

capabilities of airships. UASs are also capable of "graceful degradation", or self-destruction, if necessary.[480]

Most large UAS are remotely piloted. In current combat operations in Iraq and Afghanistan, large UASs are "controlled by pilots working in shifts and sitting in front of a video screen thousands of miles away at an air force base in America"[481] "from a console with twin video screens shaped to resemble a plane's cockpit"[482]. In contrast, BAE's HERTI can be programmed to take off, complete a full mission and land automatically.[483] Some smaller models can be carried and deployed by individuals on the ground and flown via remote control. One UAS made by Microdrone can be flown even when out of sight because it beams images from the aircraft back to video goggles worn by the operator.[484] Interested individuals can build a basic UAV for approximately $1,000 USD using Legos, a GPS unit and model aircraft parts.[485] Eick also notes that individuals can rent drones in Germany for €190 per hour.[486]

UASs being used in the civil sector have a number of specific capabilities. The US Customs and Border Protection Agency uses General Atomics' MQ-1 Predator B, which can fly between 20 and 30 hours. The Predators cost $4.5 million USD, with the accompanying ground equipment running approximately $3.5 million additional USD. Predator Bs are 36 feet long, have a wing span of 66 feet and weigh 1,500 pounds.[487] The aircraft is powered by 900 horsepower turboprop engines. A number of US police departments have also expressed an interest in using UAVs for policing. The SkySeer, manufactured by Octatron Inc and deployed by the Los Angeles Sheriff's Office, has a wingspan of 6.5 feet (1.98 m) and weighs 4 pounds (1.8 kg). The drone costs $25,000 to $30,000 USD and can fly at a speed of about 30 mph. The battery-powered drone carries out surveillance through a camera attached to the underside of the vehicle, and can incorporate low-light and infrared cameras enabling officers to find heat signatures.[488] The Miami-Dade Police Department has also acquired two Honeywell Micro Air Vehicles (MAV). This MAV weighs 14 pounds and has a maximum altitude of 10,500 feet. It has both a forward-looking and downward-looking video camera and is able to hover and continuously monitor a space. Finally, the Houston Police Department has been investigating the Insitu Insight, which has "a 10 foot wing span, a maximum altitude of 19,500 feet, and a flight endurance of more than twenty hours".[489] The Insight can carry an electro-optical camera, an infrared camera or both; however, carrying both cameras decreases the vehicle's endurance to 15 hours. In the UK, Liverpool police department has used the German AirRobot for occasional police surveillance. The AirRobot measures 3ft between the tips of its four

[480] Ollero, Aníbal, Simon Lacroix, Luis Merino, et al., "Multiple Eyes in the Skies: Architecture and Perception Issues in the COMETS Unmanned Air Vehicles Project", *IEEE Robotics & Automation Magazine*, June 2005, pp 46-57.
[481] *The Economist*, op. cit., 2007.
[482] Bowcott, Owen, and Paul Lewis, "Attack of the drones", *The Guardian*, 16 Jan 2011. http://www.guardian.co.uk/uk/2011/jan/16/drones-unmanned-aircraft
[483] Page, Lewis, "BAE in South Coast mouse-click drone spy plan: There'll be ro-birds over the white cliffs of Dover", *The Register*, 8 Nov 2007. http://www.theregister.co.uk/2007/11/08/bae_mouse_click_robot_spy_dover_over/
[484] Randerson, James, "Eye in the sky: police use drone to spy on V festival", *The Guardian*, 21 Aug 2007. http://www.guardian.co.uk/uk/2007/aug/21/ukcrime.musicnews
[485] *The Economist*, op. cit., 2007.
[486] Eick, op. cit., 2009.
[487] Matthews, William, "Border Patrol at 19,000 Feet: UAVs Take Flight Along Texas Border - During Daylight", *Defense News*, 14 June 2010. http://www.defensenews.com/story.php?i=4668081
[488] Bowes, Peter, "High hopes for drone in LA skies", BBC News, 6 June 2006. http://news.bbc.co.uk/1/hi/world/americas/5051142.stm
[489] Dunlap, op. cit., 2009, pp. 180-181.

carbon fibre rotor blades and can be fitted with CCTV cameras. MW Power, which manufactures the drone used to monitor festival-goers in the UK, is 70 cm-wide and can be fitted with high-resolution still cameras, colour video cameras and infrared night vision cameras. The battery-operated device can fly up to 500 metres high.[490] CannaChoppers have also been used by France, Switzerland and the Netherlands for large event policing and border patrol. The CannaChopper SUAVE 7 weighs 7 kg and can fly up to two hours depending on payload and fuel load. The device fits into the trunk of a car and can be transported easily.[491]

UAS fitted with electro-optical sensors "can identify an object the size of a milk carton from an altitude of 60,000 feet".[492] Both the SkySeer and the AirRobot can transmit data to a ground station, enabling an operator to see what the UAS is seeing, in real time and, if necessary, direct officers on the ground.[493] Microdrones, such as the SkySeer, can also be fitted with video cameras, thermal imaging devices, radiation detectors, mobile-phone jammers and air sampling devices.[494] One of the main advantages from UASs is that they are almost undetectable to the person(s) or target(s) being surveilled. The OPARUS project, financed by the European Commission, states that UAS can operate "almost in silence".[495] Similarly, BAE drones' flight ceiling of 20,000 feet makes them almost invisible from the ground.[496]

Applications

The Unmanned Aerial Vehicle Systems Association envisions the following potential civil or commercial applications of unmanned aircraft:

Civil or commercial applications of unmanned aircraft[497]	
Security Security and control Aerial reconnaissance Aerial policeman and crowd Monitoring Aerial traffic and security watch	**Crop management** Countryside and agriculture Agricultural activities Crop dusting
Search and rescue Maritime and mountain search and rescue Life-raft deployment Rescue point marking	**Communications** Telecommunications Telecom relay and signal coverage survey
Monitoring Civil engineering sites Waterways and shipping Oil and gas pipeline Forestry Fishery protection The countryside	**Survey** Oil and gas exploration and production Mineral exploration Geophysical surveys

[490] Randerson, op. cit., 2007.
[491] Cannachopper, "Suave 7", 2009. http://www.cannachopper.com/helicopters/47-suave7
[492] *The Economist*, op. cit., 2007.
[493] Bowes, op. cit., 2006, and Hull, Liz, "Drone makes first UK 'arrest' as police catch car thief hiding under bushes", *Daily Mail*, 12 Feb 2010. http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html#ixzz1JV7EKR1N
[494] Bowcott, Owen, and Paul Lewis, "Unmanned drones may be used in police surveillance", *The Guardian*, 24 Sept 2010. http://www.guardian.co.uk/uk/2010/sep/24/police-unmanned-surveillance-drones
[495] OPARUS, "Concept and Approach", 2010. http://www.oparus.eu/index.php/concept-a-approach
[496] Lewis, Paul, "CCTV in the sky: police plan to use military-style spy drones", *The Guardian*, 23 Jan 2010. http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones
[497] UAVS, "Civil or Commercial Applications", 2011. http://www.uavs.org/commercial

Pollution control and air sampling Crop performance Litter on beaches and in parks	
Disaster Management Disaster effects management Rescue and clear up effort supervision Disaster damage estimation	

Table 4.2: UAVS potential civil and commercial uses for UASs

Some of these applications are being used or actively explored in different countries in North America, Europe and beyond, particularly in relation to policing, border surveillance, disaster management, general regulatory surveillance and commercial applications.

Policing

With regard to policing, some police departments in Europe and North America (where data is most available) have been using UASs since approximately 2006. At least five police forces in the UK (Essex, Merseyside, Staffordshire, Derbyshire and the British Transport police) have purchased or used microdrones. The Serious Organised Crime Agency has also published a tender notice for more information about the surveillance potentials of microdrones.[498] UASs have been used by UK police to monitor festival-goers by "keep[ing] tabs on people thought to be acting suspiciously in car parks and to gather intelligence on individuals in the crowd",[499] to monitor protests at a right-wing festival[500] and to monitor the Olympic hand-over ceremony at Buckingham Palace[501]. The Merseyside police force in Liverpool has used two drones to police "public order" and "prevent anti-social behaviour". Police in Liverpool have flown the drone over groups of young people loitering in parks, as well as used it for covert surveillance.[502] Merseyside police are credited with the first UK arrest using a drone, where a car thief was tracked through undergrowth by the UASs' thermal imaging camera.[503] Once the suspect's location was detected by the AirRobot flying at 150 feet, the information was relayed to ground forces who arrested the youth. [504] A "South Coast Partnership" between Kent Police and five other police forces in the UK is seeking to use UASs for maritime surveillance as well as a range of other police issues including surveillance at the 2012 Olympic Games in London.[505] In fact, the partnership seeks to "introduce drones 'into the routine work of the police, border authorities and other government agencies' across the UK."[506] However, Lewis finds that police forces in the partnership were stressing the "good news story" of maritime surveillance rather than the general usage of UASs in police work to minimise civil liberties concerns and deflect fears about "big brother".[507]

In North America, some police forces are using or investigating the use of UASs. A North Carolina county is using UAVs with infrared cameras to monitor "gatherings of motorcycle

[498] Bowcott and Lewis, op. cit., 2011.
[499] Randerson, op. cit., 2007.
[500] Hull, op. cit., 2010.
[501] AirRobot UK, "AirRobot: The London 2012 Olympics Handover ceremony at Buckingham Palace", *AirRobot UK News*, 2008.
[502] Randerson, op. cit., 2007.
[503] Hull, op. cit., 2010.
[504] Lawrence, Mark, "Setting Matters Straight", *AirRobot UK News*, 2008. http://www.airrobot-uk.com/airrobot-news.htm
[505] Lewis, op. cit., 2010.
[506] Ibid.
[507] Ibid.

riders".[508] The UAVs fly a few hundred feet in the air, which is close enough to identify faces, and to detect marijuana fields.[509] In 2007, drones were reported over political rallies in New York and Washington, DC.[510] In Los Angeles, a sheriff's department has deployed a SkySeer drone to seek missing persons in rural areas, monitor accident or crime scenes and assist police in pursuits.[511] Additionally, Houston Police Department and Miami-Dade Police are also utilising UASs. Six police departments in Canada are using UASs in sparsely populated areas to record crime scenes and patrol smuggling corridors along the US border.[512] Canadian police are responsible for the first photographs taken by a UAV being admitted as evidence in court after the local police force used a UAV to photograph a homicide scene in 2007.[513]

In Western Europe, Eick argues that there is "hardly a marginalised group that is not targeted by UAVs". The CannaChopper has been deployed in the Netherlands and Switzerland against cannabis smokers, football fans at the European football championship in 2008 and "troublemakers" at the NATO summit in 2009.[514] The Netherlands have also used UAVs to "support police in the eviction of a squat"[515], while Belgium, France and Italy have used UASs to monitor "undocumented workers, undocumented migrants and demonstrators".[516] German Police have been using drones to monitor "alleged hooligans" and urban areas, although Eick reports that Germany is relatively "behind" other western European countries in UAS deployment.

India has also recently begun using UASs to help secure sensitive sites and events. A popular shrine that is often the target of "anti-social elements" and other security threats may get UAS surveillance.[517] Furthermore, UASs were reportedly given the "go-ahead" to assist security forces in providing surveillance coverage of games venues and residential zones during the 2010 Commonwealth Games.[518]

Border patrol

Starting in the USA in 2002, UASs have been used in border surveillance operations. The USA is one of the most well documented users of UASs in this capacity, with UAVs along the US/Mexico border and the US/Canada border. In 2002, a US Marine operated Pioneer UAV intercepted people who were attempting to smuggle 45 kg (100 lbs) of marijuana from

[508] McCullagh, Declan, "Drone aircraft may prowl U.S. skies", *CNET News*, 29 March 2006. http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746_3-6055658.html#ixzz1JURmGB4a
[509] Ibid.
[510] Whitehead, John W., *Drones Over America: Tyranny at Home*, The Rutherford Institute, Charlottesville, VA, 28 June 2010. http://www.rutherford.org/articles_db/commentary.asp?record_id=661
[511] Bowes, op. cit., 2006.
[512] Nevins, Joseph, "Robocop: Drones at Home", *Boston Review*, Jan/Feb 2011. http://www.bostonreview.net/BR36.1/nevins.php
[513] "Canadian Police Push Limits of Civilian UAV Laws", *Homeland Security News Wire*, 17 Feb 2011. http://homelandsecuritynewswire.com/canadian-police-push-limits-civilian-uavs-laws
[514] Eick, op. cit., 2009.
[515] Ibid., p. 4.
[516] Ibid., p. 4.
[517] Ians, "Tirupati temple may get UAV surveillance", *The Times of India*, 19 Oct 2010. http://articles.timesofindia.indiatimes.com/2010-10-19/india/28272904_1_tirupati-temple-uav-tirumala-tirupati-devasthanam
[518] Sarin, Ritu, "UAVs to provide real-time surveillance during Games", *Indian Express.com*, 22 Sept 2010. http://www.indianexpress.com/news/uavs-to-provide-realtime-surveillance-durin/685737/

Canada into the US.[519] In 2004-2005, UASs were deployed in routine operations along the US/Mexico border. The success of these systems is evidenced by one Predator UAV flying 886 hours and assisting officers to capture 2,300 undocumented immigrants as well as 3,760 kg (8,300 lbs) of marijuana in its first seven months.[520] In 2005, Predator UAVs along Arizona's border with Mexico were integrated into a surveillance system that included seismic sensors, infrared cameras and laser illuminators. If the seismic sensor is triggered by drug smugglers, "the Predator can investigate and, upon finding drug smugglers, tag them with its laser illuminator. With the GPS coordinates and the infrared illuminator, agents have no difficulty intercepting the smugglers".[521] The Coast Guard has also purchased 45 of Bell Helicopter's "Eagle Eye" tilt-rotor UAVs, which were planned for roll out in September 2005.[522] Austria also uses UAVs to monitor its borders[523] and Frontex, the European border agency, has held UAV demonstrations, while the UK envisions using UAS for border surveillance, particularly through maritime surveillance[524].

Environmental hazards and disaster management

UASs have also been used to monitor potential and actual environmental hazards and provide information about natural disasters. IN the US, NASA has deployed UAVs to monitor pollution and measure ozone levels, MIT is developing a GPS supported guidance systems for identifying toxins and the Department of Energy is deploying UAVs with radiation sensors to detect nuclear accidents.[525] The RAND corporation has also stated that UASs could be used "to monitor resources such as forest and farmland, wetlands, dams, reservoirs, wildlife (e.g., in nature reserves); fight fires or direct environmental remediation, with influence on food, land, water, environment, and economic development."[526] McCormack argues that UASs in Washington State in the USA could be used for "avalanche control, search and rescue, crash scene photography, land-use mapping, surveying, security inspections, hazardous material monitoring, construction data collection, aerial surveillance, and monitoring the condition and congestion of roadways."[527] In the UK, West Midlands fire service and South Wales fire service have been using drones to check the extent and spread of large fires[528], while *The Economist* reports that a UAV helped firemen monitor a recent southern California fire.[529] Other non-military uses include emissions monitoring, weather forecasting, topographical mapping, water management and traffic management.[530]

Other regulatory surveillance

UASs have also found use in relation to other civil applications. One much researched potential application is traffic monitoring, although there are significant regulatory hurdles to be

[519] Sia, Richard H.P., "Agencies see homeland security role for surveillance drones", *CongressDaily* 12 Dec 2002. http://www.govexec.com/dailyfed/1202/121202sia.htm
[520] McBride, op. cit., 2009, p. 635.
[521] Dunlap, op. cit., 2009, p. 180. See also Matthews, op. cit., 2010.
[522] Electronic Privacy Information Center, *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking, Spotlight on Surveillance*, August 2005.
http://epic.org/privacy/surveillance/spotlight/0805/
[523] Eick, op. cit., 2009.
[524] Bowcott and Lewis, op. cit., 2011 and Page, op. cit., 2007.
[525] Bolkcom, op. cit., 2004.
[526] Eick, op. cit., 2009, p. 4.
[527] McCormack, op. cit., 2008, p. 1.
[528] Randerson, op. cit., 2007 and Bowcott and Lewis, op. cit., 2011.
[529] The Economist, op. cit., 2007.
[530] Dunlap, op. cit., 2009, p. 179.

addressed before UASs can be deployed in general air space.[531] New Mexico State University with the US Coast Guard has also been exploring the use of UASs to monitor fishing regulations.[532]

Commercial applications

The market for the use of UAVs in purely commercial applications is quite nascent; however, some commercial applications are being used or explored. Interestingly, a 2000 market forecast stated that "[the] Asia Pacific...region is also at the forefront of examining a variety of civil uses of UAVs".[533] In fact, Japan is the largest user of UASs for commercial applications, principally in the form of agricultural spraying, where "robotic helicopters have been estimated to do the work of fifteen farm laborers, a necessary function due to a declining population of rice farmers in Japan."[534] Finally, there have been reports that Google is trialling UASs to support its Google Earth application.[535]

Future directions

Future directions in UAS technology primarily centre on technical developments, developments in attachments to UAVs and application developments for UASs. In terms of technical developments unrelated to the payload of UAVs, two primary developments are in evidence. The first revolves around developments in the size and shape of UAVs, or unmanned vehicles (as the case may be). These include the miniaturisation of UAVs to insect-sized surveillance vehicles that could fly through open windows[536], which is being worked on by the Air Force Research Lab, Onera, France's national aerospace centre, Harvard University and the University of Portsmouth in the UK.[537] Another innovation is "snake bot", an unmanned vehicle can be fitted with cameras or audio sensors and "slither undetected through grass and raise its head to look around, or even climb a tree for a better view".[538] Nevins further reports that research is being undertaken on a solar-powered UAV that could stay airborne for up to five years. Manufacturers are also working on making UASs more autonomous as well as trying to programme swarms of vehicles that can co-operate with one another.[539]

Other innovations revolve around the payload that can be accommodated by UASs. While most UAVs have a camera mounted on them, other payloads, particularly weapons, could be incorporated. For example, an American sheriff in South Carolina stated that "We do have the capability of putting a weapon on there if we needed to."[540] Other developments could include lethal and non-lethal weapons, such as combustible materials, incapacitating chemicals or explosives, integrated into UAV payloads[541], as could long range acoustic devices that send

[531] Srinivasan, et al., op. cit., 2004.
[532] Ibid.
[533] Herrick, Katrina, "Development of the Unmanned Aerial Vehicle Market: Forecasts and Trends", *Air and Space Europe*, Vol. 2l, No. 2, 2000, p. 27.
[534] Dunlap, op. cit., 2009, p. 179.
[535] Dillow, Clay, "Google is flying a quadcopter surveillance robot, says drone maker", *PopSci*, 9 Aug 2010. http://www.popsci.com/technology/article/2010-08/german-spy-drones-maker-sayd-google-testing-quadcopter-surveillance-drone
[536] Nevins, op. cit., 2011.
[537] The Economist, op. cit., 2007.
[538] *Wired Magazine*, quoted in Nevins, op. cit., 2011.
[539] Bowcott and Lewis, op. cit., 2011.
[540] *WLTX*, "A.I.R. (Ariel Intelligence and Response) to Help Law Enforcement", 22 Mar 2011. http://www.wltx.com/news/article/129337/2/From-Toy-to-Life-Saving-Tool
[541] Nevins, op. cit., 2011.

piercing sounds into crowds, high intensity strobe lights which can cause dizziness, disorientation and loss of balance, tasers that administer an electric shock[542] or tear gas and rubber rounds.[543] Other capabilities could include tagging targets with biological paints or micro-sensors that would enable individuals or vehicles to be tracked from afar.[544]

In relation to developments in applications, UASs could be used for a variety of new functions. Drones could be used for safety inspections, perimeter patrols around prisons and to check for cannabis being grown in roof lofts using thermal imaging.[545] They could also be used by scientists to monitor tornados, by energy companies to monitor pipelines, and/or by police to capture number plates of speeding drivers.[546] Other deployments identified by the UK newspaper, *The Guardian*, include "'[detecting] theft from cash machines, preventing theft of tractors'...railway monitoring, search and rescue... [and] to combat fly-posting, fly-tipping, abandoned vehicles, abnormal loads, waste management".[547] The development of "sense and avoid systems", which many researchers are exploring, will transform UAS technology and allow the devices to be deployed in a range of applications, potentially leading to their wide deployment.[548] Mike Heintz of the UNITE Alliance (which represents major companies such as Boeing, Lockheed Martin and Northrop Grumman) stated that further examples of UAS applications "are limited only by our imagination".[549]

4.4.3 Stakeholders and drivers driving the development of the technology

The stakeholders driving the UAS industry forward are primarily national government organisations, local public authorities/police, research laboratories and industry.

UASs are big business across the globe. In March 2011, the Teal Group predicted that the worldwide UAS market could expand to more than $94 billion USD.[550] In 2007, Eick reports that there were 259 companies that produced UAVs in 42 countries. This includes 108 companies that produced 200 UAVs in Europe, specifically 56 in France, 45 in the United Kingdom and 31 in Germany.[551] In the USA, the FAA reported that approximately 50 companies (including major names like Lockheed Martin, General Atomics Aeronautical Systems, Inc., Northrop Grumman, Boeing and Honeywell), universities and government organisations are all involved in UAV development and manufacture and are producing 155 different unmanned aircraft designs.[552] Kenzo, in 2007, discussed at least 12 different companies and universities involved in producing UAVs in Japan.[553] Furthermore, all of Europe's large aerospace and defence companies are involved in developing and manufacturing UAVs; these

[542] Whitehead, op. cit., 2010.
[543] Ibid.
[544] Nevins, op. cit., 2011 and Randerson, op. cit., 2007.
[545] Bowcott and Lewis, op. cit., 2011.
[546] Whitehead, op. cit., 2010.
[547] Lewis, op. cit., 2010.
[548] Eick, op. cit., 2009.
[549] McCullagh, op. cit., 2006.
[550] Smith, Mike, "Teal Group Predicts Worldwide UAV Market Will Total Just Over $94 Billion in Its Just Released 2011 UAV Market Profile and Forecast", *sUAS News*, 1 March 2011.
http://www.suasnews.com/2011/03/3981/teal-group-predicts-worldwide-uav-market-will-total-just-over-94-billion-in-its-just-released-2011-uav-market-profile-and-forecast/
[551] Eick, op. cit., 2009, p. 1, and Brecher, op. cit., 2003.
[552] FAA, *Fact Sheet – Unmanned Aircraft Systems (UAS)*, 1 Dec 2010.
http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=6287
[553] Nonami, op. cit., 2007.

include multi-national companies such as Thales, BAE, Sagem, Dassault, MicroDrones and AirRobot. The Israeli company Elbit is one of the best known manufacturers of UAVs.

In order to make better use of UASs in civil applications, the European Defence Agency has encouraged the European Commission to fund projects which explore further uses of UAV systems. According to the deputy chief executive of the EDA, drones are a priority for his team because of their potential applications in border control and disaster management.[554] As a result of this push, the European Union has funded various research projects to explore the potential integration of UAVs into commercial applications and general air space. These include projects such as:

- Civilian UAV thematic NETwork: technologies applications, certification (UAV-NET), 2001-2005,
- UAV Safety Issues for Civil Operators (USICO), 2002-2004,
- Civil UAV Application and Economic effectiveness of potential configuration solutions (CAPECON), 2002-2005,
- Innovative Operational UAV Integration (INOUI), 2007-2009,
- Micro Drone autonomous navigation for environment sensing (MDRONES), 2007-2009,
- Transportable Autonomous patrol for land border surveillance (TALOS), 2007-2013,
- Wide maritime area airborne surveillance (WIMAAS), 2008-2011
- Study on the Insertion of UAS in the General Air Traffic (SIGAT), 2009-2010,
- Open Architecture for UAV-based Surveillance Systems (OPARUS), 2010-2012.

These EC-funded projects are often undertaken in partnership with or between a number of arms or aerospace companies. For example, the SIGAT project is contracted to BAE Systems, Dassault Aviation, DIEHL, EADS, Sagem Defence and Security, Selex, Thales and TNO (among others).[555] While the SIGAT project has received €11.8 million in EU funding, Eick points out that between €4 and €20 million is distributed among European research networks overall.[556]

Some national governments have also become involved in supporting defence companies in developing UASs. The UK government has funded the ASTREA programme (2006-2013) which funds projects that seek to address key technological and regulatory issues to open, non-segregated airspace to UAVs.[557] Again, major companies such as BAE Systems, Thales and EADS are involved in projects within the programme, as well as large UK universities such as the Universities of Bath, Cranfield, Lancaster, Leicester and Sheffield (as well as others).[558] The Austrian Aeronautics Research and Technology Programme, financed by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT), has also funded conferences and other research work on civil applications of UAVs. Spain is funding a project called COMETS, where the University of Seville and Spain's traffic authority are working together to "improve the capabilities of UAVs in aerial missions like natural disaster

[554] Cronin, David, "Defence cuts people but spends on gadgets", *New Europe*, No. 909, 31 Oct 2010. http://www.neurope.eu/articles/Defence-cuts-people-but-spends-on-gadgets/103501.php
[555] Staicu, Marcel, "Radio Spectrum for Future UAS", *EDA Bulletin*, No. 10, Feb 2009, p. 14.
[556] Eick, op. cit., 2009, p. 6.
[557] Unmanned Aerial Vehicle Systems Association, "The ASTRAEA Programme", 2011. http://www.uavs.org/
[558] *European Business Air News*, "U.K. research into UAVs intensifies to bring forward the surveillance revolution", 6 Mar 2007. http://www.ebanmagazine.com/mag_story.html?ident=8741

remediation, traffic surveillance and law enforcement".[559] In the USA, the Department of Homeland security has pumped $10 million USD into the economy for the purchase of UAVs in border security in 2005.[560] Other stakeholders driving the development and procurement of UAVs for civil applications in the US include the House [of Representatives] Unmanned Aerial Vehicles (UAV) Caucus, DARPA, the Air Force Research Lab and the National Institute of Justice, which has helped local law enforcement organisations to acquire UASs.[561] In his worldwide roundup in 2003, Wilson also found that Iran, Turkey, India, Pakistan, South Korea, North Korea and China were all developing or purchasing UASs.[562]

Local authorities represent a second group of stakeholders who are driving the development and civil use of UASs by creating a market for them. As mentioned above, five separate police forces in the UK are using or have used UAVs in civil applications. Whitehead argues that the FAA in the US is facing pressure from state and local governments "to issue flying rights for a range of ... UAVs to carry out civilian and law-enforcement activities.[563] For example, Matthews finds that "Texans" were demanding surveillance flights over their border to protect communities from violence associated with drugs and arms trafficking.[564] The FAA states that it has been working with a number of urban police departments on test programmes to identify challenges that UASs bring as well as how to ensure the safety of operations.[565] In order to do so, they have charted an Aviation Rulemaking Committee (ARC) to produce recommendations on how to regulate small UASs. These draft rules will be published in 2011.[566]

However, industry (including industry associations) makes up the primary group of drivers of UAS integration into the civil market. Eick states that in 2006, the director of Northrop Grumman expressed concerns to the board of directors that "the decline in demand for manned aircraft posed a serious challenge for the company's future".[567] In contrast, the executive director for the Association of Unmanned Aerial Vehicle Systems International, an industry lobbying group, stated that "[UAVs] are hot".[568] Organisations such as UVS International, the Unmanned Aerial Vehicle Systems Association and the German Aerospace Industries Association are "representing" industry in its interfaces with government[569] and providing "political support" for the integration of UASs into civil applications.[570] Industry is also well represented in the European Security Research Programme, which implements a European security research programme with a fund of up to a billion euros.[571]

[559] Suman et al., op. cit., 2004, p. 131.
[560] EPIC, *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking,* Spotlight on Surveillance, August 2005. http://epic.org/privacy/surveillance/spotlight/0805/
[561] Nevins, op. cit., 2011.
[562] Wilson, op. cit., 2003.
[563] Whitehead, op. cit., 2010.
[564] Matthews, op. cit., 2010.
[565] FAA*, Fact Sheet – Unmanned Aircraft Systems (UAS)*, 1 Dec 2010.
http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=6287
[566] Ibid.
[567] Eick, op. cit., 2009, p. 4.
[568] Sia, op. cit., 2002.
[569] Unmanned Aerial Vehicle Systems Association, "About us", 2011. http://www.uavs.org/
[570] Eick, op. cit., 2009.
[571] Hayes, Ben, *Arming Big Brother: the EU's security research programme, Summary of the report*, Transnational Institute, April 2006. http://www.tni.org/es/archives/act/4451

Beneficiaries

Not surprisingly, the stakeholders who are driving the use of UASs in civil air space, governments, local authorities and industry, are also the primary beneficiaries of integrating UASs into civil air space. Manufacturers of UASs have significantly benefited from European and national government spending on UAS systems, where Nevins finds that UAS manufactures have received $20 billion USD in Pentagon spending in the last 10 years, while the CIA and Congress have also invested billions.[572] Governments and local authorities find that procuring and running UAS represents a significant cost savings compared with manned aircraft.[573] For example, *The Economist* reports that operating a small helicopter can cost upwards of $1,000 per hour while a drone is a fraction of that.[574] However, Matthews cautions that while UASs may be less expensive to buy, they can be more expensive to operate because of the number of support personnel needed.[575] Another benefit of UASs is that they do not put pilots at risk. Furthermore, the capabilities of UASs offer significant benefits. Bolkcom states that UASs' loiter capabilities, their ability to track violators with thermal detection sensors and their endurance means that "illegal border entrants" are more likely to be caught and there is a decreased burden on human resources.[576] Furthermore, smaller UAVs can fly under the weather and much closer to the ground; they can fly at higher speeds than ground vehicles and they can monitor large areas.[577]

4.4.4 Privacy impacts and ethical issues raised by the technology

While there are clear beneficiaries in relation to the deployment of UASs in civil applications, industry experts, academics, CSOs and journalists all voice significant concerns about the large-scale deployment of UASs, particularly in relation to safety, ethics and, more specifically, privacy.

Safety

Safety is a primary consideration for individuals commenting on the possibility of large-scale deployments of UASs. Bolkcom reports that the current accident rate for UAVs is 100 times that of manned aircraft[578], which EPIC argues increases risks to commercial aircraft and civilians on the ground.[579] Also, UASs may be less well maintained and subsequently, less reliable than manned aircraft.[580] In 2007, the US National Transportation Safety Board (NTSB) reported that pilot error was the cause of an April 2006 Predator B crash, as the team piloting the UAV accidentally turned the engine off.[581] There is also a serious risk that UAVs, particularly as payloads become more sophisticated, could be used as a weapon.[582] For example,

[572] Nevins, op. cit., 2011.
[573] Bolkcom, op. cit., 2004; Page, op. cit., 2007; *Strategic Comments*, op. cit., 2009; Eick, op. cit., 2009; Bowcott and Lewis, op. cit., 2010; and Coifman, Benjamin, Mark McCord, Rabi G. Mishalani and Keith Redmill, "Surface Transportation Surveillance from Unmanned Aerial Vehicles", *Proceedings of the 83rd Annual Meeting of the Transportation Research Board*, 2004. http://www.ceegs.ohio-state.edu/~coifman/documents/UAV_paper.pdf
[574] *The Economist*, op. cit., 2007.
[575] Matthews, op. cit., 2010.
[576] Bolkcom, op. cit., 2004.
[577] Coifman, et al., op. cit., 2004.
[578] Bolkcom, op. cit., 2004.
[579] EPIC, op. cit., 2005.
[580] Dunlap, op. cit., 2009.
[581] *The Economist*, op. cit., 2007.
[582] Coifman, et al., op. cit., 2004.

despite interest in using UASs to monitor the 2012 Olympic Games, *The Guardian* reports that the CAA is unlikely to allow UASs so close to large crowds and London City Airport.[583]

Ethics

There are also significant ethical considerations surrounding the use of UASs in civil applications. There has been an on-going debate around the ethics of using remotely piloted vehicles in combat operations. They have been blamed for significant losses of life on the ground in combat zones, the removal of soldiers "from the human consequences of their actions".[584] The foundation of the International Committee for Robot Arms Control (Icrac) in 2009 marked the beginning of a protest movement against such "armed autonomous robots".[585] In relation to civil applications, Hayes, of Big Brother Watch, states that "drones and other robotic tools will add to the risks of a Playstation mentality developing along Europe's borders."[586] Whitehead argues that drones view everyone as a suspect because "[e]veryone gets monitored, photographed, tracked and targeted".[587] Similarly, Nevins notes that while UASs are seen by law enforcement as "just another tool in the toolbox" and technologically neutral, "[t]here is every reason to be concerned about how the law enforcement and 'homeland security' establishments will take advantage of their new tools".[588] Whitehead concurs, stating that technology functions without discrimination and that "the logical aim of technologically equipped police who operate as technicians must be control, containment and eventually restriction of freedom".[589] Hayes further argues that the European Union's security-industrial complex has placed law enforcement demands ahead of civil liberties concerns.[590] Nevins agrees, stating that "the normalization of previously unacceptable levels of policing and ... official abuse" has "disturbing implications for civil and human rights". Nevins also reports fears of "mission creep" in police use of UASs.[591] These ethical concerns become intertwined with safety concerns as the potential for UASs to carry weapons, including non-lethal weapons, draws nearer. Whitehead reports that a spokesman for PrisonPlanet.com, a well-known civil liberties website, stated that the death toll from non-lethal tasers in the US is over 350 people, and warns that this could skyrocket if the "personal element of using a taser is removed and they are strapped to marauding surveillance drones".[592]

Privacy

While the above section discussed general concerns around civil liberties, privacy emerges as one of the key civil liberties stakeholders are concerned about in relation to the deployment of UASs. Some journalists have relayed worries about the distinct lack of concern about the potential for civil liberties intrusions by UASs. Nevins quotes Stephen Graham, Professor of Cities and Society at Newcastle University, who says that "broader concern about the regulation and control of drone surveillance of British civilian life has been notable by its ab-

[583] Bowcott and Lewis, op. cit., 2011.
[584] Cronin, op. cit., 2010.
[585] Bowcott and Lewis, op. cit., 2011.
[586] Hayes, Ben, *Arming Big Brother: the EU's security research programme, Summary of the report*, Transnational Institute, April 2006. http://www.tni.org/es/archives/act/4451
[587] Whitehead, op. cit., 2010.
[588] Nevins, op. cit., 2011.
[589] Whitehead, op. cit., 2010.
[590] Hayes, op. cit., 2006.
[591] Nevins, op. cit., 2011.
[592] Whitehead, op. cit., 2010.

sence."[593] Evidence from projects on UASs suggests that the focus of web materials, reports and deliverables is on the technical capabilities and potential applications of UASs and they only mention privacy in passing.[594] Similarly, when discussing the revocation of the LA sheriff's licence to deploy UASs, Killam briefly mentions ACLU concerns about the surveillance of private citizens.[595]

Yet a number of journalists and other stakeholders have made concerted efforts to raise or relay privacy issues in relation to UASs. A report in *The Economist* notes that "UAVs can peek much more easily and cheaply than satellites and fixed cameras can"; they can "hover almost silently above a property" and that "the tiny ones that are coming will be able to fly inside buildings".[596] *The Economist* also quotes an FAA spokesman who stated that "It smacks of Big Brother if every time you look up there's a bug looking at you".[597] In *The Guardian*, a Professor of Robotics at Sheffield University stated that it was necessary to have a public consultation about the use of UASs; individuals could be facing a future where "someone gets Tasered from the air for dropping litter, or even for relieving themselves down an alleyway under cover of night".[598] EPIC notes that UAVs give the US federal government "a new capability to monitor citizens clandestinely" and states that the costs of these vehicles may outweigh the benefits.[599] Liz Hull of *The Daily Mail* also reports that UASs are a "worrying extension of Big Brother Britain,"[600] while Sia in *CongressDaily* reports that the Senate Armed Services Committee Chairman acknowledged that UASs are "quite intrusive"[601]. Other journalists also note that specific victims of the mass deployment of UASs in civil air space could be celebrities who are subject to paparazzi drones.[602]

Some of the consequences of the intrusions of UASs include physical, psychological and social effects. For example, McBride notes that conventional surveillance aircraft, such as helicopters, provide auditory notice that they are approaching and allow a person "to take measures to keep private those activities that they do not wish to expose to public view".[603] McBride also argues that the mass deployment of UAS surveillance vehicles which are imperceptible from the ground "could lead to an environment where individuals believe that a UAS is watching them even when no UASs are in operation".[604] This could have a self-governing effect, as first described by Bentham and Foucault, where individuals adjust their behaviour as though they were being watched at all times.[605] As a result, Dunlap argues, "this advancement of surveillance technology threatens to erode society's expectation of privacy, just as the airplane once erased individuals' expectations of privacy in their fenced-in backyards."[606]

---

[593] Nevins, op. cit., 2011.
[594] McCullagh, op. cit., 2006; OPARUS, op. cit., 2010; Nevins, op. cit., 2011.
[595] Killam, Tim, "US Perspective on Unmanned Aerial Vehicles", Institution of Engineering and Technology, 5 Dec 2007.
[596] *The Economist*, op. cit., 2007.
[597] Ibid.
[598] Randerson, op. cit., 2007.
[599] EPIC, op. cit., 2005.
[600] Hull, op. cit., 2010.
[601] Sia, op. cit., 2002.
[602] Bowcott and Lewis, op. cit., 2011.
[603] McBride, op. cit., 2009, p. 659.
[604] Ibid., p. 661.
[605] Foucault, Michel, *Discipline and Punish: The Birth of the Prison*, Vintage, New York, 1977.
[606] Dunlap, op. cit., 2009, p. 202.

While some have argued that privacy concerns represent a significant stumbling block to the large-scale deployment of UASs, others have argued that UAS surveillance is no different from current surveillance technologies and methods. Brecher, for example, states that privacy concerns are a near-term barrier to the deployment of UAVs but argues that this can be mitigated by highlighting the benefits of this science and technology development to the public.[607] In the US, local law enforcement officials have also recognised that privacy concerns represent a stumbling block to the deployment of UASs; however, they have sought to assure the public that "they will not be spied upon by these unmanned drones" and that "this is not [sic] different than what police have been doing with helicopters for years".[608] In LA, police officials reminded citizens that "There's no place in an urban environment that you can go to right now that you're not being looked at with a video camera".[609] While in the UK, senior police officials have argued that "unmanned aircraft are no more intrusive than CCTV cameras and far cheaper to run than helicopters."[610] Similarly, in relation to reports that Google has acquired a UAS, Dillow argues that although "adding an aerial surveillance drone to the mix could stir the ire of privacy advocates", "[i]t's tough to make a case that shooting photos on a public street is an invasion of privacy".[611]

4.4.5 Extent to which the existing legal framework addresses the privacy impacts

The numerous, relevant concerns around the safety, ethics and privacy impacts of UASs demonstrate that the use of these devices needs to be regulated. Broadly speaking, there are currently "no regulations at the European or national levels for the commercial use of Unmanned Aerial Vehicles" and this lack of regulation is a significant barrier to their deployment in civil applications.[612] The Aircraft Owners and Pilots Association states that governments need to define what a UAV is and they need to integrate UAVs into the current air-space system. Part of the difficulty in drawing up regulatory parameters for the use of UASs is that UAVs span an entire spectrum between model aircraft and manned aerial vehicles such as planes and helicopters. Some UAVs are comparable to "large jet-powered machines capable of flying across the Atlantic", while micro-UAVs are more closely related to remote control model aircraft.[613] This means that UAS regulations will likely vary depending on the model, size, weight and speed, making regulations significantly complex and difficult to understand and enforce. Large UASs that incorporate sense-and-avoid systems (i.e., systems that detect other aircraft or flying objects and enables a UAS to avoid them) would be comparatively easy to regulate due to their similarity with manned aircraft. However, *The Economist* warns that, "[b]elow a certain size, unmanned aircraft could be impossible to regulate".[614]

Safety regulations

Currently, UASs in civil air space are regulated by various national authorities. While there is a dearth of English language information about other countries, the Federal Aviation Authority in the US[615], the Civil Aviation Authority in the UK, the Civil Aviation Safety Authority

[607] Brecher, op. cit., 2003.
[608] Dunlap, op. cit., p. 182.
[609] Bowes, op. cit., 2006.
[610] Lewis, op. cit., 2010.
[611] Dillow, op. cit., 2010.
[612] Eick, op. cit., 2009, p. 5.
[613] *The Economist*, op. cit., 2007.
[614] *The Economist*, op. cit., 2007.
[615] FAA, op. cit., 2010.

in Australia, Transport Canada, regional authorities in Germany and the European Aviation Safety Agency all provide some regulatory information. One problem, as Coifman et al. note, is that in many countries and the US in particular, there is an "alphabet soup" of organisations that have some jurisdiction over UASs.[616] One major problem blocking the integration of UASs into general air space is the absence of "sense and avoid" systems built into UASs.[617] Other issues include communication systems and weather avoidance systems.[618] Until solutions to these problems are available, the civil use of UAVs is likely to be operationally constrained and segregated from manned aircraft.[619] However, in the meantime, many airport authorities confer Certificates of Approval or other similar measures to enable temporary flights of UASs.[620]

Privacy regulations

As Dunlap points out, even if civil operators, such as law enforcement, are able to purchase a UAS and obtain necessary authorisation from the FAA, CAA or other national or regional aviation authority, activities such as surveillance will still confront fundamental rights obstacles such as the United States Constitution or the European Charter of Fundamental Rights.[621] As stated in section 2, many law enforcement organisations have argued that there is no distinct difference between surveillance by UAS and surveillance by other vehicles such as helicopters which police have been using for some time. This section focuses on the tension between the deployment of UAS for law enforcement purposes and the various privacy regulations with which they may come into conflict. It focuses specifically on discussions of case law around the US Fourth Amendment and the European Court of Human Rights.

The Fourth Amendment of the US Constitution protects citizens from unreasonable searches, particularly in areas where individuals have a reasonable expectation of privacy, such as their home or the curtilage (i.e., yard or garden) of their home. Case law has set a precedent where searches are considered unreasonable if a person exhibited a reasonable expectation of privacy, and if that expectation is one which society also recognises as reasonable.[622] Dunlap states that a US Supreme Court Justice has argued that "a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited".[623] As a result, officers have been able to act on information that they gleaned "from naked-eye observations"[624] and "the Fourth Amendment has never required police officers 'to shield their eyes when passing by a home'."[625] This includes material or activities that are visible to the naked eye from aerial vehicles such as helicopters and airplanes, due to the fact that the airways are "public" and that "any member of the public could fly over [a per-

[616] Coifman, et al., op. cit., 2004.
[617] Haddon and Whittaker, op. cit., 2004.
[618] Bolkcom, op. cit., 2004.
[619] Haddon and Whittaker, op. cit., 2004, p. 1.
[620] See, FAA, op. cit., 2010; Directorate of Airspace Policy, op. cit., 2010, p. 2; Civil Aviation Safety Authority of Australia, "Unmanned Aerial Vehicle (UAV) Operations, Design Specification, Maintenance and Training of Human Resources", Advisory Circular AC 101-1(0), July 2002, p. 16. http://www.casa.gov.au/wcmswr/_assets/main/rules/1998casr/101/101c01.pdf ; Transport Canada, "Unmanned Air Vehicle", 3 May 2010. http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm and UAVS, "Airspace Regulation", 2011. http://www.uavs.org/regulation
[621] Dunlap, op. cit., 2009.
[622] Dunlap, op. cit., 2009, p. 185.
[623] Ibid.
[624] McBride, op. cit., 2009, p. 627.
[625] Dunlap, op. cit., 2009, p. 186.

son's] backyard and observe" illegal materials or activity.[626] Furthermore, in *California vs. Ciraolo*, where the defendant was convicted of growing marijuana plants as a result of photographs from an airplane secured by the police, the Supreme Court also ruled that the use of a normal 35mm camera in the operation did not constitute an unreasonable search because it used photographic technology that is "generally available to the public"[627] and the flight itself was judged to be "routine".[628]

However, the opinion of the Court did reflect the possibility that the use of technology which was not generally available to the public might constitute an unreasonable search. For example, the Court stated that "[a]erial observation of curtilage may become invasive, either due to physical intrusiveness or though modern technology which discloses to the senses those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens."[629] Thus, the court ruled that obtaining information about activities inside a home via thermal imaging cameras "constitutes a search – at least where (as here) the technology in question is not in general public use".[630]

Thus, both McBride and Dunlap find that, as long as UASs are not in "general public use", their use for surveillance in places where individuals have a reasonable expectation of privacy would be covered by the Fourth Amendment and the police would be required to obtain a search warrant prior to their use. This is further true if the flights were not considered "routine", for example, if they were flying at non-routine altitudes.[631] However, both point out that if ever UASs are in "general public use", this protection would be nullified. One danger surrounding the general usage principle is that UAVs that could see through "windows or skylights would not constitute a search if the activities or objects inside could be seen with the naked eye" if they were in general use.[632] Furthermore, because electro-optical lenses function similarly to binoculars, telescopes and conventional cameras already used by the public, these sorts of searches could be constitutional even if UASs themselves were not in general public usage.[633] In a similar vein, the courts could argue that UASs are similar enough to helicopters and other methods already used by the police to make surveillance of the area outside the home constitutional.[634]

In Europe, the use of aerial surveillance technologies is covered by the Charter of Fundamental Rights of the European Union 2000. Article 7 of the Charter of Fundamental Rights states that a person has a right to respect for their private and family life, home and communications, while Article 8 states that an individual has the right to the protection of their personal data. This protection of personal data includes fair processing, consent, access to data and right to rectification. In *Peck vs. the United Kingdom*, the European Court of Human Rights reiterated an understanding that "the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life", making public space sur-

[626] Ibid., p. 186-187.
[627] Ibid., p. 189.
[628] McBride, op. cit., 2009.
[629] McBride, op. cit., 2009, p. 649.
[630] Dunlap, op. cit., 2009, p. 195, and McBride, op. cit., 2009, p. 655.
[631] McBride, op. cit., 2009, p. 647.
[632] Dunlap, op. cit., 2009, p. 199.
[633] Ibid.
[634] Ibid.

veillance such as CCTV lawful under the Charter of Fundamental Rights.[635] Under this consideration, UAS surveillance that monitors but does not record would be lawful. However, public space surveillance which does record visual data would be considered "personal data" under the CFREU and would mean subjects have rights of access and correction. This is the case in current deployments of visual surveillance systems, such as CCTV, in the UK, where the Data Protection Act 1998 stipulates that individuals must be told that a surveillance system is in operation and individuals can request copies of the data the CCTV data controller holds about them.[636] However, it would be difficult to inform individuals that UAS surveillance is in operation, particularly as one of the advantages to UAS surveillance is that they are silent and fly at altitudes which make them practically invisible.

4.4.6 Need for new legislation, codes of conduct etc. to deal with privacy impacts not covered by the existing framework

Future-oriented rules and regulations surrounding the use of UASs suggest ways to mitigate concerns around privacy in the deployment of UASs for civil applications. Suggestions for future-oriented privacy standards have primarily come in the form of the relationship between UAS surveillance and the Fourth Amendment in the US. McBride and Dunlap have argued that the technological capabilities of UASs mean that their relationship with the Fourth Amendment must be explicitly examined. McBride states that UAS surveillance should be considered "presumptively unconstitutional" because UASs *require* technology to undertake visual surveillance, and the benefits of UASs are specifically associated with high powered cameras, thermal imaging cameras and other sensors. [637] Thus, the future regulation of warrantless UAS surveillance should try to differentiate the features of UAS surveillance from conventional aerial surveillance.[638] Dunlap states that rather than focusing on the legality of the flights under the FAA or other regulatory authorities:

> Congress, state legislatures, and federal and state executive agencies must craft rules that would ensure that domestic law enforcement agencies do not employ UASs to engage in conduct that violates the Fourth Amendment and erodes the privacy expectations of the people. Although law enforcement agencies claim that they have no intention of spying on people in their homes, there must be some oversight and external direction to instruct police departments on the proper usage of these powerful aerial observers. These legislative and administrative measures should also restrict the technological devices that can be mounted on UASs or, at least, define the situations when they can be utilized by law enforcement.[639]

In Europe, Big Brother Watch have concurred and argued that "stringent, clear, and easily accessible guidelines about how and when these drones can be deployed".[640]

4.4.7 Discussion

In order for UASs to be utilised for civil applications, they must offer stringent and comprehensive protections of citizens' fundamental rights. Specifically, they must conform to the European Charter of Fundamental Rights, where individuals' private and family lives are re-

---

[635] Williams, Victoria, "Privacy Impact & the Social Aspects of Public Surveillance", *Covert Policing Review*, 2008.
[636] Information Commissioners Office, CCTV Code of Practice, Wilmslow, Cheshire, UK, 2008.
[637] McBride, op. cit., 2009, p. 655.
[638] Ibid., p. 651.
[639] Dunlap, 2009, p. 203
[640] Sharpe, Dylan, "Surveillance drone grounded days after 'success'", *Big Brother Watch*, 16 Feb 2010. http://www.bigbrotherwatch.org.uk/home/2010/02/surveillance-drone-grounded-days-after-success.html

spected and where they can expect protections around their personal data. As UASs are arguably similar to both public space surveillance, such as CCTV, and targeted surveillance, such as helicopter surveillance, rules and regulations must either take account of the context in which UASs are deployed or be drafted to ensure comprehensive protections for individual personal data. For example, UASs that are deployed for general public space surveillance, as is currently being considered in relation to the 2012 Olympic Games, should conform to the protections outlined by the UK Information Commissioners Office, where individuals are notified that UASs are in operation and individuals can request access to their data. However, UASs which are deployed for targeted and potentially covert surveillance operations may require search warrants or other legal or institutional approval before the action is carried out. This is particularly the case as UASs can be both silent and invisible. Finally, UASs for civil applications should not incorporate weapons, particularly given the potential for disconnection that could lead to a "Playstation mentality" about which Ben Hayes of Big Brother Watch has raised concerns.

4.5 CONCLUSION

An investigation of these new technologies of surveillance suggests that existing regulatory principles do not offer adequate protection of individuals' fundamental rights. Whole body imaging scanners raise significant issues in terms of individual privacy, particularly in places such as the UK where individuals are not given alternatives to undergoing body scans. Further concerns surround individuals of certain religious groups, those who have disabilities and vulnerable individuals such as children and pregnant women. However, a range of different organisations have suggested a combination of PETs, industry standards, codes of practice and legislation that could offer robust protections for individual privacy.

The discussion around unmanned aircraft systems is significantly less detailed. While there are potentials for privacy breaches, these have been less well covered, possibly due to the similarities between UAV surveillance and current public space surveillance methods such as helicopters and CCTV systems. However, a number of academics have argued that the protections that individuals enjoy in relation to these current methods should be extended to the use of UAVs. In particular, that targeted surveillance activities should require warrants or other official approvals, or, that generalised public space surveillance should be undertaken with full awareness of the general public, and should conform to data protection principles.

4.6 REFERENCES

Body Scanners

Abeyratne, Ruwantissa, "Full body scanners at airports—the balance between privacy and state responsibility", *Journal of Transportation Security*, Vol. 3, 2010, pp. 73–85.

airport-technology.com, "TSA Approves L-3's ProVision Millimeter Wave Checkpoint Screening System", 4 Dec 09. http://www.airport-technology.com/contractors/security/l-3_security/press35.html

airport-technology.com, "Cook County Selects L-3 ProVision™ Whole Body Imaging Solution for Deployment across Large Prison Complex", 10 Feb 09. http://www.airport-technology.com/contractors/security/l-3_security/press22.html

American Civil Liberties Union, "ACLU Continues To Receive Complaints About New Airport Screening Procedures", 2 Dec 2010. http://www.aclu.org/national-security-technology-and-liberty/aclu-continues-receive-complaints-about-new-airport-screeni

ACLU, “NYCLU Sues State Department of Corrections for Information about Controversial Method for Screening Prison Visitors for Drugs”, 26 May 2010. http://www.aclu.org/drug-law-reform-prisoners-rights-technology-and-liberty/nyclu-sues-state-department-corrections-info

ACLU, “ACLU Submits Statement On Aviation Security To Key Senate Committees”, Jan 20 2010. http://www.aclu.org/national-security-racial-justice-technology-and-liberty/aclu-submits-statement-aviation-security-key

ACLU, “Backgrounder on Body Scanners and ‘Virtual Strip Searches’”, 8 Jan 2010. http://www.aclu.org/technology-and-liberty/aclu-backgrounder-body-scanners-and-virtual-strip-searches

ACLU, “The ACLU's view on body scanners”, 15 Mar 2002. http://www.aclu.org/technology-and-liberty/body-scanners

Article 29 Data Protection Working Party, *Response to Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection*, 11 May 2009.

AS&E, “Privacy-Enhanced Smartcheck”, 2011. http://www.as-e.com/products_solutions/smartcheck_privacy.asp

Associated Press, “NY Sen. Seeks Bill to Deter Body Scan Image Misuse”, *The New York Times*, 5 Dec 2010. http://www.nytimes.com/aponline/2010/12/05/us/AP-US-Airport-Security.html?hp

Associated Press, “Dutch to use full body scanners for U.S. flights”, *MSNBC.com*, 30 Dec 2009. http://www.msnbc.msn.com/id/34630097/ns/us_news-airliner_security/

BBC News, “'Naked' scanner in airport trial”, 13 Oct 2009. http://news.bbc.co.uk/1/hi/uk/8303983.stm;

Blake, Heidi, “Full body scanners may break child pornography laws”, *The Telegraph*, 5 Jan 2010. http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/6933898/Full-body-scanners-may-break-child-pornography-laws.html

Cavoukian, Ann, *Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy*, Information and Privacy Commissioner Ontario, Canada, March 2009.

CBC News, “Airport scanners invade privacy: advocate”, 5 Jan 2010. http://www.cbc.ca/canada/british-columbia/story/2010/01/05/bc-airport-scanners-civil-liberties-vonn.html

Cendrowicz, Leo, “Can Airport Body Scanners Stop Terrorist Attacks?”, *TIME Magazine*, Jan 05, 2010. http://www.time.com/time/world/article/0,8599,1951529,00.html#ixzz1IBr9lbM3

Centre for European Policy Research, “Body Scanners”, IN:EX Roundtable, 27 Jan 2011. http://www.ceps.eu/content/proceedings-selection-inex-meetings

Clark, Pilita, “How airport body scanners will be used”, *Financial Times*, 30 Dec 2009. http://www.ft.com/cms/s/0/4c4887ec-f594-11de-90ab-00144feab49a,dwp_uuid=f39ffd26-4bb2-11da-997b-0000779e2340.html

Conroy, Michael, “How the ProVision 'naked airport scanner' works”, *Wired.co.uk*, 14 May 2010. http://www.wired.co.uk/magazine/archive/2010/06/start/how-the-provision-naked-airport-scanner-works

Deane, Alexander, “Better Safe?”, *IPA Review*, June 2010.

Department for Transportation, *Impact Assessment on the use of security scanners at UK airports*, 29 Mar 2001.

Department of Homeland Security, *Privacy Impact Assessment for TSA Whole Body Imaging*, 17 Oct 2008. http://epic.org/privacy/body_scanners/DHS_PIA_08_17_08.pdf

DSE International, “EOD305 Handheld Passive Millimeter Wave Scanner”, 2011. http://www.dseinternational.com/content/products/Product.aspx?Id=216

EDRi-gram, “The European Parliament says no to airport body scanners”, No. 6.21, 5 Nov 2008.

Electronic Privacy Information Center (EPIC), “EPIC v. Department of Homeland Security - Body Scanners”, 25 March 2011. http://epic.org/privacy/airtravel/backscatter/epic_v_dhs.html

EPIC, “Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding”, June 2005. http://epic.org/privacy/surveillance/spotlight/0605/

Ernst and Young, “France”, *Update IP/ICT Legal Practice*, No. 5, Oct 2010.

Etzioni, Amitai, “Private Security: In defense of the 'virtual strip-search'”, *The New Republic*, 9 Oct 2010. http://www.tnr.com/article/politics/78250/private-security-virtual-strip-search

European Commission, Commission communication on the use of security scanners at European airports — questions and answers, MEMO/10/261, Brussels, 15 June 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/261&format=HTML&aged=0&language=EN&guiLanguage=e

European Commission, Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports COM(2010) 311/4 , Brussels, 2010.

European Commission, Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, Brussels, 19 Feb 2009. http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm

European Economic and Social Committee, Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM(2010) 311 final, Brussels, 16 Feb 2011.

European Parliament, Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, RSP/2008/2651, 2008. http://www.europarl.europa.eu/oeil/FindByProcnum.do?lang=en&procnum=RSP/2008/2651

Fay Joe, “EU bottoms up committee slates body scanners: Expensive, flaky, not fit for purpose ...”, *The Register*, 17 Feb 2011. http://www.theregister.co.uk/2011/02/17/scanner_opinion/

Goodin, Dan, “Skeletal scanner would ID terrorists from 50 meters: And maybe non-terrorists too”, *The Register*, 24 Aug 2010. http://www.theregister.co.uk/2010/08/24/skelital_image_scanner/

Haines, Lester, “Heathrow security man cops perv scanner eyeful”, *The Register*, 24 Mar 2010. http://www.theregister.co.uk/2010/03/24/heathrow_body_scanner/

Health Physics Society, “American National Standard N43.17: Radiation Safety For Personnel Security Screening Systems Using X-rays”, 09 July 2010. http://www.hps.org/hpssc/N43_17_2002.html

Heussner, Ki Mae, “Air Security: Could Technology Have Stopped Christmas Attack?”, *ABC News*, 29 Dec. 2009. http://abcnews.go.com/Technology/AheadoftheCurve/air-security-technology-stopped-xmas-attack/story?id=9436877

Hrejsa, Allen F., and Morris L. Bank, “The use of low dose x-ray scanners for passenger screening at public transportation terminals should require documentation of the ‘in-

formed consent' of passengers", *Medical Physics*, Vol. 32, No. 3, March 2005, pp. 651–653.
JetSetCD, "Updated: What Airports Have Full-Body Scanners Right Now", *Jaunted*, 2 Mar 2010. http://www.jaunted.com/story/2010/3/1/232031/9854/travel/Updated%3A+What+Airports+Have+Full-Body+Scanners+Right+Now
Kessler, Mary Elaine, and Brett R. Seeley, "Predicting the Impact of Full Body Scanners on Air Travel and Passenger Safety", Naval Postgraduate School, MBA Professional Report, June 2010.
Klitou, Demetrius, "Backscatter body scanners – A strip search by other means", *Computer Law & Security Report*, Vol. 24, Issue 4, 2008, pp. 316-325.
Kravitz, Derek, "Are airport X-ray machines catching more than naked images?", *The Washington Post*, 26 Dec 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/12/25/AR2010122502277.html?hpid=topnews
Mordini, Emilio, *Whole Body Imaging at airport checkpoints: the ethical and political context*, HIDE&RISE policy report, February 2010 (updated March 2011). www.riseproject.eu
L-3 Communications, "TSA to Test L-3 Millimeter Wave Portals at Phoenix Sky Harbor Airport", 11 Oct 2007. http://www.l-3com.com/news-events/pressrelease.aspx?releaseID=1061924
Mackey, David A., "The 'X-Rated X-Ray': Reconciling Fairness, Privacy, and Security", *Criminal Justice Studies*, Vol. 20, No. 2, June 2007, pp. 149–159.
Mason, Wyatt, "Scanners Gone Wild", *The New York Times*, 3 Dec 2010. http://www.nytimes.com/2010/12/05/magazine/05FOB-wwln-t.html?ref=technology
Mellor, Chris, "US airport body scanners can store and export images", *The Register*, 12 Jan 2010. http://www.theregister.co.uk/2010/01/12/tsa_body_scanners/
Millivision, "Millivision Technologies Threat Detection Systems", 2009. http://www.millivision.com/
Millivision, "Portal System 350: Turnkey Threat Detection", 2009. http://www.millivision.com/portal-350.html
Millivision, "Stand-Off System 350: Unobtrusive Threat Detection", 2009. http://www.millivision.com/stand-off-350.html
Millivision, "Walk-By System 350: Efficient Threat Detection", 2009. http://www.millivision.com/walk-by-350.html
Millward, David, "Passengers who refuse scanner face flying ban", *The Telegraph*, 1 Feb 2010. http://www.telegraph.co.uk/travel/travelnews/7129835/Passengers-who-refuse-scanner-face-flying-ban.html
Mironenko, Olga, "Body scanners versus privacy and data protection", *Computer Law & Security Review*, Vol. 27, No. 3, 2011, pp. 232-244.
Office of the Privacy Commissioner of Canada, "Letter in response to the Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA) in anticipation of the deployment of millimetre wave (MMW) screening technology at selected Canadian airports", 29 Oct 2009. http://www.priv.gc.ca/pia-efvp/let_20100108_e.cfm
OPC of Canada, Annual Report to Parliament 2008-2009, Report on the Privacy Act. http://www.priv.gc.ca/information/ar/200809/200809_pa_e.cfm.
Peterson, Rohen, "The Emperor's New Scanner: Muslim Women at the Intersection of the First Amendment and Full Body Scanners", *Social Science Research Network*, 6 Mar 2010. http://ssrn.com/abstract=1684246

Privacy International, *Germany - Privacy Profile*, 26 Jan 2011. https://www.privacyinternational.org/article/germany-privacy-profile
Privacy International, *Norway - Privacy Profile*, 23 Jan 2011. https://www.privacyinternational.org/article/norway-privacy-profile
Privacy International, *France - Privacy Profile*, 22 Jan 2011. https://www.privacyinternational.org/article/france-privacy-profile
Privacy International, "PI statement on proposed deployments of body scanners in airports", 31 Dec 2009. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-565802&als[theme]=Border%20and%20Travel%20Surveillance
Quinn, Ben, "Why Europe doesn't want an invasion of body scanners", *Christian Science Monitor*, 26 Jan 2010. http://www.csmonitor.com/World/Europe/2010/0126/Why-Europe-doesn-t-want-an-invasion-of-body-scanners
Ramachandran, Arjun, "X-ray security: can airport system be hacked?", *Sydney Morning Herald*, 7 Jan 2010. http://www.smh.com.au/technology/technology-news/xray-security-can-airport-system-be-hacked-20100107-lvyq.html
Rapiscan Systems, "Backscatter / Rapiscan Secure 1000 Single Pose", 2011. http://www.rapiscansystems.com/rapiscan-secure-1000-single-pose.html
Rapiscan Systems, "Backscatter / Rapiscan Secure 1000 Dual Pose", 2011. http://www.rapiscansystems.com/rapiscan-secure-1000.html
Rosen, Jeffrey, "Nude Awakening", *The New Republic*, 29 Jan 2010. http://www.tnr.com/article/politics/nude-awakening;
Rucker, Philip, "US airports say seeing is believing as passengers face body-scan drill", *Sydney Morning Herald, 5 Jan 2010.* http://www.smh.com.au/travel/travel-news/us-airports-say-seeing-is-believing-as-passengers-face-bodyscan-drill-20100104-lq6o.html
Schiphol Airport Security, *Security Scan Brochure*. http://www.schiphol.nl/Travellers/AtSchiphol/CheckinControl/SecurityChecksUponDeparture/SecurityScan.
Schwartz, John, "Debate Over Full-Body Scans vs. Invasion of Privacy Flares Anew After Incident", *The New York Times*, 29 Dec 2009. http://www.nytimes.com/2009/12/30/us/30privacy.html
Smiths Detection, "People screening systems", 2011. http://www.smithsdetection.com/millimeter-wave_inspection.php
Tek84 Engineering Group, "Body Scanner", 2011. http://www.tek84.com/bodyscanner.html
The Telegraph, "Airport body scanners 'may be unlawful'", 15 Feb 2010. http://www.telegraph.co.uk/travel/travelnews/7242087/Airport-body-scanners-may-be-unlawful.html
Transport Commission, Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, 19 Feb 2009. http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm
Transportation Security Administration, "Advanced Imaging Technology (AIT)", 2011. http://www.tsa.gov/approach/tech/ait/index.shtm
The TSA Blog, "More on Passive Millimeter Wave Technology", 5 Sept 2008. http://blog.tsa.gov/2008/09/more-on-passive-millimeter-wave.html
Travis, Alan, "Anti-terror body scanners may be illegal, ministers warned", *The Guardian*, 16 Feb 2010. http://www.guardian.co.uk/uk/2010/feb/16/uksecurity-terrorism
Unique Scan, "Custom clothing and apparel", 2011. http://www.uniquescan.com/
United Press International (UPI), "Airliner attack re-ignites scanner debate", 29 Dec 2009. http://www.upi.com/Top_News/Special/2009/12/29/Airliner-attack-re-ignites-scanner-debate/UPI-98181262114910/

Venier, Sylvia, “Global Mobility and Security”, *Biometric Technology Today*, May 2010, pp. 7-10.
Weinberger, Sharon, “Airport security: Intent to deceive?”, *Nature*, Vol. 465, 26 May 2010, pp. 412-415. http://www.nature.com/news/2010/100526/full/465412a.html
W*elt Online,* “EU lawmakers criticize ‘virtual strip search’”, 23 Oct 2008. http://www.welt.de/english-news/article2614271/EU-lawmakers-criticize-virtual-strip-search.html;
Wikipedia.org, “Full body scanner”, 2011. http://en.wikipedia.org/wiki/Full_body_scanner
Xinhua, “China's new body scanner debuts, promises privacy”, 21 Apr 2011. http://news.xinhuanet.com/english2010/china/2011-04/21/c_13840130.htm
Zetter, Kim, “Airport Scanners Can Store, Transmit Images”, *Wired News*, 11 January 2010. http://www.wired.com/threatlevel/2010/01/airport-scanners/

UAVs

AirRobot UK, “AirRobot: The London 2012 Olympics Handover ceremony at Buckingham Palace”, *AirRobot UK News*, 2008.
Bolkcom, Christopher, *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance*, Congressional Research Service Report for Congress, 28 June 2004.
Bowes, Peter, “High hopes for drone in LA skies”, *BBC News*, 6 June 2006. http://news.bbc.co.uk/1/hi/world/americas/5051142.stm
Bowcott, Owen, and Paul Lewis, “Attack of the drones”, *The Guardian*, 16 Jan 2011. http://www.guardian.co.uk/uk/2011/jan/16/drones-unmanned-aircraft
Bowcott, Owen, and Paul Lewis, “Unmanned drones may be used in police surveillance”, *The Guardian*, 24 Sept 2010. http://www.guardian.co.uk/uk/2010/sep/24/police-unmanned-surveillance-drones
Brecher, Aviva, “Roadmap to near-term deployment of unmanned aerial vehicles (UAV) for transportation applications charge to participants”, *UAV 2003: Roadmap for Deploying UAVs in Transportation Specialist Workshop*, 2 Dec 2003, Santa Barbara, California.
Cannachopper, “Suave 7”, 2009. http://www.cannachopper.com/helicopters/47-suave7
Civil Aviation Safety Authority of Australia, “Unmanned Aerial Vehicle (UAV) Operations, Design Specification, Maintenance and Training of Human Resources”, Advisory Circular AC 101-1(0), July 2002. http://www.casa.gov.au/wcmswr/_assets/main/rules/1998casr/101/101c01.pdf
Coifman, Benjamin, Mark McCord, Rabi G. Mishalani and Keith Redmill, “Surface Transportation Surveillance from Unmanned Aerial Vehicles”, *Proceedings of the 83rd Annual Meeting of the Transportation Research Board*, 2004. http://www.ceegs.ohio-state.edu/~coifman/documents/UAV_paper.pdf
Cronin, David, “Defence cuts people but spends on gadgets”, *New Europe*, No. 909, 31 Oct 2010. http://www.neurope.eu/articles/Defence-cuts-people-but-spends-on-gadgets/103501.php
Department of Homeland Security, “Canadian Police Push Limits of Civilian UAV Laws”, *Homeland Security News Wire*, 17 Feb 2011. http://homelandsecuritynewswire.com/canadian-police-push-limits-civilian-uavs-laws
Dillow, Clay, “Google is flying a quadcopter surveillance robot, says drone maker”, *PopSci*, 9 Aug 2010. http://www.popsci.com/technology/article/2010-08/german-spy-drones-maker-sayd-google-testing-quadcopter-surveillance-drone
Directorate of Airspace Policy, *CAP 722: Unmanned Aircraft System Operations in UK Airspace – Guidance*, Civil Aviation Authority, 6 Apr 2010.

Dunlap, Travis, “Comment: We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search”, *South Texas Law Review*, Vol. 51, No. 1, Fall 2009, pp. 173- 204.

The Economist, “Unmanned aircraft: The fly's a spy”, 1 Nov 2007. http://www.economist.com/displaystory.cfm?story_id=10059596

Eick, Volker, *The Droning of the Drones: The increasingly advanced technology of surveillance and control*, Statewatch Analysis, No. 106, 2009. http://www.statewatch.org/analyses/no-106-the-droning-of-drones.pdf

Electronic Privacy Information Center, *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking, Spotlight on Surveillance*, August 2005. http://epic.org/privacy/surveillance/spotlight/0805/

European Business Air News, “U.K. research into UAVs intensifies to bring forward the surveillance revolution”, 6 Mar 2007. http://www.ebanmagazine.com/mag_story.html?ident=8741

Federal Aviation Administration, *Fact Sheet – Unmanned Aircraft Systems (UAS)*, 1 Dec 2010. http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=6287

FH Joanneum University of Applied Sciences, “Unmanned Aircraft Systems - Towards Civil Applications”, Graz, Austria, 10 Nov 2009. http://www.fh-joanneum.at/aw/home/Studienangebot_Uebersicht/fachbereich_information_design_technologien/lav/news_events_ordner_lav/Archiv/~btch/lav_news_091110/?lan=de

Foucault, Michel, *Discipline and Punish: The Birth of the Prison*, Vintage, New York, 1977.

Haddon, D.R., and C.J. Whittaker, *UK-CAA Policy for Light UAV Systems*, UK Civil Aviation Authority, 28 May 2004.

Hayes, Ben, *Arming Big Brother: the EU's security research programme, Summary of the report*, Transnational Institute, April 2006. http://www.tni.org/es/archives/act/4451

Herrick, Katrina, “Development of the Unmanned Aerial Vehicle Market: Forecasts and Trends”, *Air and Space Europe*, Vol. 2l, No. 2, 2000.

House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State, Vol. 2*, HL Paper 18, Second Report, Session 2008-09, House of Lords, London, 6 Feb 09.

Hull, Liz, “Drone makes first UK 'arrest' as police catch car thief hiding under bushes”, *Daily Mail*, 12 Feb 2010. http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html#ixzz1JV7EKR1N

Ians, “Tirupati temple may get UAV surveillance”, *The Times of India*, 19 Oct 2010. http://articles.timesofindia.indiatimes.com/2010-10-19/india/28272904_1_tirupati-temple-uav-tirumala-tirupati-devasthanam

Information Commissioners Office, CCTV Code of Practice, Wilmslow, Cheshire, UK, 2008.

Killam, Tim, “US Perspective on Unmanned Aerial Vehicles”, Institution of Engineering and Technology, 5 Dec 2007.

Lawrence, Mark, “Setting Matters Straight”, *AirRobot UK News*, 2008. http://www.airrobot-uk.com/air-robot-news.htm

Lewis, Paul, “CCTV in the sky: police plan to use military-style spy drones”, *The Guardian*, 23 Jan 2010. http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones

Matthews, William, “Border Patrol at 19,000 Feet: UAVs Take Flight Along Texas Border - During Daylight”, *Defense News*, 14 June 2010. http://www.defensenews.com/story.php?i=4668081

McBride, Paul, “Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations”, *Journal of Air Law and Commerce*, Vol. 74, 2009.

McCormack, Edward D., *The Use of Small Unmanned Aircraft by the Washington State Department of Transportation*, Washington State Transportation Center, June 2008.
McCullagh, Declan, "Drone aircraft may prowl U.S. skies", *CNET News*, 29 March 2006. http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746_3-6055658.html#ixzz1JURmGB4a
Nevins, Joseph, "Robocop: Drones at Home", *Boston Review*, Jan/Feb 2011. http://www.bostonreview.net/BR36.1/nevins.php
Nonami, Kenzo, "Prospect and Recent Research and Development for Civil Use Autonomous Unmanned Aircraft as UAV and MAV", *Journal of Systems Design and Dynamics*, Vol. 1, No. 2, 2007, pp. 120-128.
Ollero, Aníbal, Simon Lacroix, Luis Merino, et al., "Multiple Eyes in the Skies: Architecture and Perception Issues in the COMETS Unmanned Air Vehicles Project", *IEEE Robotics & Automation Magazine*, June 2005, pp. 46-57.
OPARUS, "Concept and Approach", 2010. http://www.oparus.eu/index.php/concept-a-approach
Page, Lewis, "BAE in South Coast mouse-click drone spy plan: There'll be ro-birds over the white cliffs of Dover", *The Register*, 8 Nov 2007. http://www.theregister.co.uk/2007/11/08/bae_mouse_click_robot_spy_dover_over/
Randerson, James, "Eye in the sky: police use drone to spy on V festival", *The Guardian*, 21 Aug 2007. http://www.guardian.co.uk/uk/2007/aug/21/ukcrime.musicnews
Sarin, Ritu, "UAVs to provide real-time surveillance during Games", *Indian Express.com*, 22 Sept 2010. http://www.indianexpress.com/news/uavs-to-provide-realtime-surveillance-durin/685737/
Sharpe, Dylan, "Surveillance drone grounded days after 'success'", *Big Brother Watch*, 16 Feb 2010. http://www.bigbrotherwatch.org.uk/home/2010/02/surveillance-drone-grounded-days-after-success.html
Sia, Richard H.P., "Agencies see homeland security role for surveillance drones", *CongressDaily* 12 Dec 2002. http://www.govexec.com/dailyfed/1202/121202sia.htm
Smith, Mike, "Teal Group Predicts Worldwide UAV Market Will Total Just Over $94 Billion in Its Just Released 2011 UAV Market Profile and Forecast", *sUAS News*, 1 March 2011. http://www.suasnews.com/2011/03/3981/teal-group-predicts-worldwide-uav-market-will-total-just-over-94-billion-in-its-just-released-2011-uav-market-profile-and-forecast/
Srinivasan, Sumanm, Haniph Latchman, John Shea, Tan Wong and Janice McNair, "Airborne Traffic Surveillance Systems: Video Surveillance of Highway Traffic", *Proceedings of the ACM 2nd international workshop on Video surveillance & sensor networks*, 2004, pp. 131–135.
Staicu, Marcel, "Radio Spectrum for Future UAS", *EDA Bulletin*, No. 10, Feb 2009.
Strategic Comments, "The drones of war", Vol. 15, No. 4, 2009, pp. 1-2.
Transport Canada, "Unmanned Air Vehicle", 3 May 2010. http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm and
Unmanned Aerial Vehicle Systems Association, "About us", 2011. http://www.uavs.org/
UAVS, "Airspace Regulation", 2011. http://www.uavs.org/regulation
UAVS, "The ASTRAEA Programme", 2011. http://www.uavs.org/
UAVS, "Civil or Commercial Applications", 2011. http://www.uavs.org/commercial
UAVS, "UAV or UAS?", 2011. http://www.uavs.org/index.php?page=what_is
Whitehead, John W., *Drones Over America: Tyranny at Home*, The Rutherford Institute, Charlottesville, VA, 28 June 2010. http://www.rutherford.org/articles_db/commentary.asp?record_id=661

Williams, Victoria, “Privacy Impact & the Social Aspects of Public Surveillance”, *Covert Policing Review*, 2008.
Wilson, J.R., “UAVs: A Worldwide Roundup”, *Aerospace America*, June 2003. https://www.aiaa.org/aerospace/Article.cfm?issuetocid=365&ArchiveIssueID=39
WLTX, “A.I.R. (Ariel Intelligence and Response) to Help Law Enforcement”, 22 Mar 2011. http://www.wltx.com/news/article/129337/2/From-Toy-to-Life-Saving-Tool

Chapter 5 – Second-generation Biometrics

Silvia Venier and Emilio Mordini,
Centre for Science Society and Citizenship

5.1 INTRODUCTION TO THE FIELD

As a result of global trends such as the emergence of a borderless economy as well as of international security threats, improved measures for strong identification of individuals have been and are continuously being developed and applied worldwide. Biometric identification technologies have gained prominence in recent decades and have replaced many conventional identification methods based on passwords, smart cards or tokens as an automated, more secure and convenient way of identify individuals.

The widespread use of biometrics has been made possible by explosive advances in computer science and by the "near universal connectedness of computers around the world"[641]. On the other hand, biometrics are still a "young and promising technology"[642], and it is often said that the future of biometrics involves their ability to adapt to ever more challenging situations. Due to important qualitative technical advances, nowadays many speak of the emergence of biometrics of a "second-generation". Key elements of these developments are the emergence of new biometric traits (the so called *behavioural*, *physiological* and *soft* biometrics) often used in combination with more traditional traits (in *multiple biometrics* or *multimodal systems*). The shift to embedded systems, where biometric technologies could support the broader trends towards ambient intelligence or ubiquitous computing, is another new element. The potential for revealing very sensitive (e.g. health, race, emotional state) information and the covert data capture without the subject consent are among the most controversial aspects of these emerging technologies.

Biometric identification has long been the subject of public debate, ethical reflection and regulatory efforts. Many elements of this next generation biometrics are, however, giving rise to a new set of ethical, legal and socio-political issues that have not yet been discussed in depth. This paper seeks to contribute to this debate. Section two gives a brief overview of biometric systems, addressing the state of the art of second-generation biometrics. Next, it focuses on the main drivers and barriers for the deployment of second-generation biometrics (section three) and on their current and potential applications (section four). It then elaborates on the impact of second-generation biometrics on society, on their ethical and privacy issues (section five) and on the gaps within the existing legal framework (section six). The last section is devoted to possible options for future global governance of current and future biometric systems (section seven).

5.2 CURRENT STATUS OF SECOND-GENERATION BIOMETRICS AND EXPECTED PROGRESS

5.2.1 Overview of biometric systems

A biometric is a measurable physical, physiological or behavioural trait that can be used to automatically recognise an individual. Biometric recognition is based on some fundamental premises of this specific body trait, such as collectability (it can be measured), universality (it exists in all persons), permanence (its properties remain stable over time) and uniqueness (it must be distinctive to each person). Performance criteria include the level of accuracy and

[641] See Nanvati, Samir, Michael Thieme and Raj Nanavati, *Biometrics: identity verification in a networked world*, Wilety Ltd, 2002.

[642] European Biometrics Portal - UNISYS, *Biometric in Europe: Trend Report,* June 2006, http://www.libertysecurity.org/IMG/pdf/Trend_Report_2006.pdf

suitability for recognition purposes of the human attribute, the speed of recognition and resistance to circumvention of a given biometric system, as well as the factors that influence user's acceptability[643]. Biometrics represent a highly reliable means of authentication because they provide a stronger connection between individuals and their alleged identity. The most widely used traditional biometrics for identification purposes include fingerprint-based recognition systems (probably the most popular method[644]), hand geometry[645], iris scan[646] and face recognition[647]. The range of body features that can be used for biometric recognition has greatly expanded since the technology was first developed. It has also been said that today any personal feature would appear to be biometric measurable[648], even if with varying degrees of reliability.

Biometric identification processes usually involve four stages: enrolment, storage, acquisition and matching. The first time an individual uses a biometric system is called *enrolment*. During this phase, biometric data is collected using a sensor, in order to produce a biometric *template* (i.e. the digital representation, a binary mathematical file) of the sample which is then stored in a portable medium, such as a smart card, or in a centralised database (*storage* phase). The next time the individual presents his body trait to the system, the acquired template (*acquisition* phase) is compared to the enrolled template using a mathematical algorithm to see if they match (*matching*). This matching is a statistical process: the algorithm provides a score of the degree of similarity between the two templates being compared and the final decision is regulated by a threshold determining the margin of error allowed by the algorithm. The threshold level can be adjusted according to the application requirements.

Biometric information can be stored both as an *encrypted template* (digital representation of a biometric characteristic) and as a *raw image* (analogical representation). A raw image can facilitate the interoperability of biometric systems, since it can be inputted into a different system without the need to re-enrol the user[649]. On the other hand, encrypted templates offer a greater security as it can be extremely difficult to reconstruct the original biometric image

[643] Seven properties have been presented as being shared by all biometric modalities: universality, distinctiveness, permanence, collectability, performance, acceptability, resistance to circumvention. These seven pillars provide a tool for the analysis of all biometric systems. See Jain, Anil K., Ruud Bolle and Sharath Pankanti, *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publisher, Massachusetts, USA, 1999.

[644] Since the early 1900s, fingerprints have been accepted method of forensic investigations to identify suspects. Nowadays, nearly all law enforcement agencies worldwide use Automatic Fingerprint Identification System (AFIS), that became first available in the mid 1970s. In the very last decades, the use of fingerprint modality has been increasingly extended to cover also some civilian and commercial applications.

[645] One of the first applications of hand geometry was the INPASS system (Immigration and naturalization service system), installed at some of the major airports in the US in the mid 1990s, and later abandoned due to its limited user enrolment and weaker performance.

[646] An excellent survey on current iris recognition technologies is available in Bowyer, Kevin, Karen Hollingsworth and Patrick J. Flynn, "Image Understanding for Iris biometrics: a survey", *Computer Vision and Image Understanding*, Vol. 110, No. 2, 2008, pp. 281-307.

[647] Research in this field has been on-going since 1960s. Current approaches are based on two dimensional (2D) and three dimensional (3D) images, or even infrared facial scans. See Zhao W., Chellappa, R., Phillips, P., J., Rosenfeld, A., "Face recognition: a literature survey", *ACM Computing Surveys*, Vol. 35, No. 4, Dec 2003, pp. 399–458.

[648] Commission de l'Ethique, de la Science et de la Technology in Québec, *In search of balance: an ethical look at new surveillance and monitoring technologies for security purposes*, Position Statement, 2008.

[649] International Civil Aviation Organisation Technical Advisory Group (ICAO TAG), *Biometrics Deployment of Machine Readable Travel Documents*, ICAO TAG MRTD/NTWG Technical Report, 2004.

from them[650]. Digital templates can also help to alleviate concerns about the derivation of additional sensitive information from the collected biometric data.

Almost all uses of biometrics can be classified into one of the two modes: *verification* (or authentication, that implies confronting the person with the identity he claims in order to verify this claim) and *identification* (that usually implies confronting the person with a great number of identities, in order to establish what identity can legitimately be associated with a person)[651]. Verification is a one-to-one comparison of a captured biometric with a stored template (1:1 matching), while during the identification process a captured biometric is compared against a database of thousands or even millions of other templates in search of a match, in a one-to-many comparison (1:N matching).

The choice to use a particular biometrics for verification or identification purposes depends mainly on its robustness, the accuracy of the recognition, and the requirements of the intended application (high or low security, large scale or not). For instance, fingerprint, face and iris, which are amongst the most popular physical characteristics collected, have sufficient discriminating power to be applicable in large-scale identification applications. On the contrary, the discriminatory power of hand geometry or voice is quite limited and these systems are mainly employed for verification purposes and in low security access control applications. Different types of storage (local or centralised) also depend on the overall objective of the system: identification (and screening-based applications) requires a centralised database, while verification-based applications can use either central or local storage.

Biometric identification systems are not perfect systems, since they are subject to errors and circumventions. Biometric systems are subject to errors due to external factors, such as environmental conditions (lighting, temperature, noise) or human factors (pose, facial expression, stress and fatigue patters, medical conditions[652]). Working on the basis of a probabilistic methodology, errors are intrinsic to any biometric system. The performance of a biometric system is analysed thought the measurement of the *failure to enrol rate* (FTE), *false acceptance rate* (FAR, the probability that a system incorrectly matches the captured biometric with the stored template, creating a false positive) and *false rejection rate* (FRR, the probability that the system fails to detect a match, creating a false negative). For a given biometric system, it is not possible to simultaneously reduce the FAR and the FRR, and a trade-off between FAR and FRR is always necessary. The equal error rate (EER) represents the rate at which both FAR and FRR are equal. In general, the lower the EER, the more accurate the system is. In addition to intrinsic failures, the security of a system can also be voluntarily compromised. A number of studies have analysed the likelihood of security breaches unique to biometrics (such as spoofing[653], replay or substitution attacks[654] and tampering[655]), in addition to attacks

[650] The digital representation of biometric data is said to be irreversible, meaning that from a template it is not possible to deduce the biometric data themselves. For a comprehensive analysis on this topic see Yanushkevich Svetlana, Adrian Stoica, Vlad Shmerko and Denis Popel, *Biometric Inverse Problems*, CRC Press, Boca Raton, 2005.

[651] The picture of human recognition modes is completed by *detection* (to detect the presence of a human being is usually a preliminary task in order to identify the person) and *screening* (also called *negative identification*, since the aim is to recognise a person as not being part of a given list of individuals). See Mordini, Emilio, *ACTIBIO Ethical Manual*, ACTIBIO D8.1, 2009. http://www.actibio.eu:8080/actibio/files/document/Deliverables/ACTIBIO_Deliverable_8.1.pdf

[652] See below for a more detailed description of the links between biometric identification and health conditions.

[653] A fake biometric is used to spoof the system.

[654] Replay attack is where an image is recorded and inserted into the system by an intruder. A substitution attack occurs when the intruder replace the right template with a different template.

that are typical of any information system. For this reason, the development of multi-biometric systems, as well as the use of anti-spoofing and aliveness detection technologies is increasingly becoming an essential component of biometric identification[656]. Various standards models have also been developed as protection profiles for biometric systems[657]. The unsatisfactory performance of biometric technologies acquired in less than ideal conditions has limited their deployment in a considerable way. Scholars agree that a significant improvement in recognition performance in uncontrolled situations is one of the main challenges of future biometrics. Standardisation and interoperability complete the picture of current and future technical challenges for traditional biometric systems that are increasingly developed and used worldwide.

5.2.2 State of the art of second-generation biometrics

While the examples of traditional biometrics mentioned above are *mature technologies* that have found applications in a wide range of law enforcement, civilian and commercial systems, the expression "second-generation biometrics" generally refers to a group of biometric technologies that are *still in the research domain*[658], or at least not yet sufficient mature for deployment and inappropriate for large scale applications or high security purposes. This is mainly due to technological as well as costs limitations.

This section deals with the analysis of the state of the art of "second generation biometrics". A preliminary clarification on the terminology used is needed. As said in the previous section, the main aim of any biometric system is to provide a reliable way of recognising an individual from a *physical* or *behavioural* body trait. The measurement of human "behaviour" is thus already included into the general definition of "biometrics". However, the expression "second" or "next-generation biometrics" is increasingly being used with reference to emerging trends in biometric systems, with new body traits being collected and used for categorisation of individuals, sensors being developed that can allow the collection of such traits from a distance or on the move, and potentially new deployments of such systems that go from profiling and surveillance practices to ambient intelligence and smart environment applications. Most techniques of second-generation biometrics perform personal recognition using a dynamic approach, i.e. they collect dynamic (or behavioural) characteristics. One of the defining characteristics of behavioural biometrics is thus the incorporation of the time dimension into the recognition process. Acquiring such characteristics is often possible due to improved sensors

[655] The attacker modifies the feature sets to ensure that a high match score is achieved.
[656] For a comprehensive analysis of spoofing attacks see Buhan, Ileana, and Pieter Hartel, "The state of the art in abuse of biometrics", University of Twente Internal Report, 2005. http://eprints.eemcs.utwente.nl/722/01/00000144.pdf
[657] These are: the Biometric Device Protection profile (BDPP, issued in September 2011 by the UK government biometrics working group), the US Department of Defence & Federal Biometric Systems Protection Profiles for Medium Robustness Environment (DoDPP, developed in March 2002), the US government biometric verification mode protection profile for medium robustness environments (USGovPP, issued in November 2003). Recently a new standard has been published by ISO (ISO/IEC 24745:2011 Information Technologies – Security techniques – Biometric information protection, issued in August 2011).
[658] Some types of biometrics, although categorised as "second-generation", are much older than those referenced as "first-generation". Well-known examples include hand signature, voice recognition or the so called "lie detector".

network capabilities[659] and to advances in sensor technologies that can collect new human characteristics[660].

A commonly agreed categorisation of behavioural biometrics is yet to be established[661]. Generally speaking, the following groups are usually mentioned: biometrics based on the measurement of "motor skills" (i.e. the ability of a human being to utilise muscles), on the measurement of electromagnetic body signals, on the measurement of human-machine interaction patterns.

Motor-skills: biometric recognition is based on the measurement of one or more physical parameters over time.

TECHNOLOGY	STATE OF THE ART and EMERGING TRENDS
Gait recognition (analysis of walking patterns)[662]	The main challenge in gait recognition research is in the specification of some gait features that are sufficiently *discriminable* and can be reliably extracted from video. Recent studies on the gait recognition potential are focused mainly in two directions: view-invariant gait analysis and novel algorithm for the extraction and fusion of static and kinematic parameters of human locomotion[663]. In the last decade, gait as a biometric has received greater attention due to increase in the importance of surveillance and security in public and private areas. A novel gait recognition system has recently been developed and tested in the scope of the EU funded HUMABIO project[664]. Building on the results of HUMABIO, other potential uses of gait recognition were investigated in the EU funded ACTIBIO project[665].
Dynamic facial features, eye blinking, lip move-	Dynamic facial feature methods are based on the tracking of the motion of skin pores during an expression to obtain a vector field that characterises

[659] Networked sensors have been introduced in smart environments that are capable to detect physical and motion-based properties.

[660] Such as, for instance, a new generation of olfactory sensors that can collect body odours. For an overview of new sensors see Cook, Diane, "Prediction algorithms for smart environments", in "Smart environments: technologies, protocols and applications", in Diane Cook and Sajal Das (eds.), *Series on parallel and distributed computing*, Wiley, 2004, pp. 175-192.

[661] For a comprehensive overview of 2nd generation biometric existing research, see Wang Lai-Xi, X. Geng, "Behavioural biometrics for human identification: intelligent applications", *Medical Information Science Reference*, IG Global, 2009; for a more complete taxonomy and classification of the various types of behavioural biometrics see Yampolskiy, Roman and Venu Govindaraju, "Behavioural biometrics: a survey and classification", *International Journal of Biometrics*, Vol. 1, No. 1, 2008, pp. 81 – 113.

[662] See Sakar S., P. J. Phillips, Z. Liu, I. R. Vega, P. Groter P and K. W. Bower, "The Human ID Gait challenge problem: data sets, performance, and analysis", *IEEE transactions on pattern analysis and machine intelligence*, Vol. 27, No. 2, 2005, pp. 162 – 177.

[663] See Ioannidis Dimosthenis, Dimitrios Tzovaras, Gabriele Dalle Mura, Marcello Ferro, Gaetano Valenza, Alessandro Tognetti and Giovanni Pioggia, "Gait and Anthropometric profile biometrics: a step forward", in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press. The main challenge in gait recognition research is in the specification of some gait features that are sufficiently *discriminable* and can be reliably extracted from video.

[664] HUMABIO, Human monitoring and authentication using biodynamic indicators and behavioural analysis, http://www.humabio-eu.org

[665] ACTIBIO, Unobtrusive Authentication using ACTivity related and soft biometrics, http://www.actibio.eu:8080/actibio

[666] Pamudurthy Satpren, E., Guan, Klaus Mueller and Miriam Raifilovich, "Dynamic approach for face recognition using digital image skin correlation", State University of New York, 2005.

TECHNOLOGY	STATE OF THE ART and EMERGING TRENDS
ments	the deformation of the face[666]. A system for identifying users by analysing voluntary blink patterns has also recently been developed[667]. Attempts have been made to generate a model representing lip dynamics produced by a person during speech[668].
Voice recognition (analysis of vocal behaviour)[669]	Voice is a particular feature that involves a combination of physiological (the shape and size of the relevant body components) and behavioural traits (the ways these components move). Voice can be employed for either speaker identification or authentication, and can be considered as one of the best-researched biometric technologies. This technology is very usable and it is widely accepted by the public.
Signature/handwriting[670] or other authorship based biometrics	Signature verification (both through static/offline and dynamic/online methods) is a widely accepted methodology for confirming identity. The hand-written signature dynamics can be seen as less intrusive than other biometric technologies. Authorship based biometrics are based on observing style peculiarities typical to the author of the work being examined (such as text, painting, but also software programming). Emerging trends of authorship based biometrics include sketch recognition[671], e-mail behaviour[672], programming style[673].

Body signals: traditionally used in medicine, this category refers to electromagnetic signals emitted by the human body.

[667] See Westeyn Tracy, Peter Pesti, Kwang-Hyun Park and Thad Starner, "Biometric identification using song-based eye blink patterns", *Human Computer Interaction International*, HCCI, Las Vegas NV, 2005. http://www.cc.gatech.edu/~thad/p/031_30_Gesture/biometric_ID_HCII05.pdf

[668] Shipilova, Olga, *Persons recognition based on lip movements*, 2004. http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Shipilova.pdf

[669] For an updated analysis of speaker recognition research see Faundez Zanui, Marcos and Monte Moreno, "State of the art in speaker recognition", *IEEE Aerospace and Electronic System magazine*, Vol. 20, No.5, 2005, pp. 7-12.

[670] For an overview on the state of the art see Gupta, Gopal, *The State of the Art in On-line Handwritten Signature Verification*, Faculty of Information Technology, Monash University, Clayton, Victoria, Australia, May 2006.

[671] See Stephan Al-Zubi, Arslan Brömme and Klaus D. Tönnies. "Using an Active Shape Structural Model for Biometric Sketch Recognition", in *Proceedings of DAGM-Symposium,* 2003, pp.187-195.

[672] Stolfo, Salvatore, Chia Wei Hu, Wei-Jen Li, Shlomo Hershkop, Ke Wang, Olivier Nimesken, *Combining behavioural models to secure email systems*, Columbia University Technical report, 2003.

[673] With the increasing number of viruses worms etc, the author of such malware programs can be identified through the analysis of the source code. See Spafford, Eugene H., and Stephen A. Weeber, "Software forensics: can we track code to its authors?", Purdue University Technical Report, 1992.

TECHNOLOGY	STATE OF THE ART AND EMERGING TRENDS
Electrocardiogram (ECG, records the electromagnetic signals produced by the heart as measured on the skin) Electroencephalogram (EEG, records the electromagnetic signals generated by the brain as measured on the scalp) Electrooculogram (EOG, records eye movements) Electromyogram (EMG, records muscle activity)	These systems can record the electronic signals naturally emitted by the heart, the nervous system or the eye. This category includes also the analysis of muscle activity. Electrophysiological biometrics are universal and very difficult to fake. The main difference with other behavioural biometrics is the data that are acquired: specialised hardware and highly obtrusive equipment are required in order to acquire biological signal data. Emerging trends: EEG and ECG were included among the modalities used in the pilot tests of the above mentioned HUMABIO project[674].

Other examples of "body signals" used as biometric characteristics suitable for recognition purposes include the analysis of the respiratory rate, the temperature profile of the face (facial thermography), signs of trepidation. Particularly researched biometrics based on body signals also include:

TECHNOLOGY	STATE OF THE ART AND EMERGING TRENDS
body odour recognition[675]	Research has demonstrated that is feasible to recognise humans on the basis of their body odour. This could however be complicated by the use of deodorants and perfumes. Instruments capable of distinguishing invariant components of human odour have been recently developed[676].
skin luminescence	With its dermal thickness and subcutaneous layers, human skin produces distinctive reflections when lights are shown through it. Skin luminescence could be useful as an aliveness-detection methodology in multimodal systems.
vein pattern technology	Blood vessels authentication is a very secure authentication method and is difficult to counterfeit. There are several pilot applications ranging from physical access control to ATM cash dispensers (the latest mainly in Japan).

Human-computer interaction (HCI): these systems measure how human beings interact with machines

TECHNOLOGY	STATE OF THE ART AND EMERGING TRENDS
Human computer interaction	These systems explore how human beings interact with computational devices, and include direct and indirect methods. Direct methods are based on direct human interactions (such as keystroke or mouse dynamics). Indirect methods analyse

[674] http://www.humabio-eu.org

[675] Studies to use body odour as a biometric identification technology are being carried out by the department of homeland security - see Shaun Waterman, UPI special report, "DHS wants to use human body odour as biometric identifier, clue to deception", March 2009. http://www.upi.com/Top_News/Special/2009/03/09/DHS-wants-to-use-human-body-odor-as-biometric-identifier-clue-to-deception/UPI-20121236627329

[676] See Keller, Paul, "Overview of electronic nose algorithm", *International Joint Conference of Neural Networks,* Washington, DC, 1999; Korotkyaya, Zhanna, "Biometric person authentication: odor", report in *Advanced topics in Information Processing,* University of Technology, Finland, 2003.

TECHNOLOGY	STATE OF THE ART AND EMERGING TRENDS
	events produced unintentionally by the user (program execution traces[677], network traffic, registry access[678] and storage activity[679]).
Measurement of advanced behaviours	These systems measure advanced human behaviours (such as strategy, skills or knowledge) exhibited by the user during interaction with different software. As an example, a statistical model of players' strategies in various games (including online games) may be used to detect imposters[680].

Although particular efforts are increasingly devoted to behavioural biometrics, the majority of biometrics research is still aimed at studying traditional physical characteristics. Because of the technological advances introduced, some advanced traditional biometrics are often referred to as biometrics of "next-generation", the most researched being:

TECHNOLOGY	STATE OF THE ART AND EMERGING TRENDS
Advanced facial recognition (next-generation of face recognition that includes 3D and infrared systems) [681]	Today, face recognition has achieved a quite high performance rate. Implementing 3D face recognition, to a certain extent solves the issue of 2D face recognition being highly dependent on lighting, pose and expressions. Currently, standards are being deployed to include 3D facial images in e-Passports. Even if algorithms have not yet achieved the level of robustness typical of human face recognition for highly familiar faces, with unfamiliar faces the difference in accuracy might be less pronounced[682]. A relevant current field of research is devoted to facial expressions that are produced in response to felt emotions.

[677] Gosh, Anup K., Aaron Schwartzbard and Michael Schatz, "Learning program behaviour profiles for intrusion detection", *Proceedings of the first USENIX workshop on intrusion detection and network monitoring*, Santa Clara, California, 1999.

[678] Apap, Frank, Andrew Honig, Shlomo Hershkop, Eleazar Eskin and Sal Stolfo, *Detecting malicious software by monitoring anomalous windows registry access*, Columbia University CS Technical Report, 2001

[679] Pennington, Adam, John Strunk, John Linwood Griffin, Craig Soules, Garth Goodson and Gregory Ganger, *Storage-based intrusion detection: watching storage activity for suspicious behaviour*, Technical Report CMU-CS-02-179, Carnegie Mellon University, 2002.

[680] This can be very important in massive online games involving real money trading. See ENISA "Survey on security issue in virtual words", October 2008. http://www.enisa.europa.eu/act/it/oar/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/survey-on-security-issues-in-virtual-worlds

[681] An excellent survey of existing face recognition systems is available at Andrea Abate, Michele Nappi, Daniel Riccio and Gabriele Sabatino, "2D and 3D face recognition: a survey", *Pattern recognition letters*, Vol.28, No. 14, 2007, pp. 1885-1906.

[682] Tistarelli, Massimo, Susan E. Barret and Alice O'Toole, "Face Recognition, Emotion and Intention Detection: The Big Brother in the Airport?", in Mordini, Emilio, and Dmitrios Tzovaras, *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.

TECHNOLOGY	STATE OF THE ART AND EMERGING TRENDS
Remote iris scan (iris captured at a distance) [683]	An algorithm for automated iris recognition was developed in the early 1990. Due to the high universality, uniqueness, and stability over time, irises are among the most used biometric traits for identification. Currently, iris recognition systems are in place at a number of US, Canadian and EU airports. Although, in general user cooperation is essential for iris recognition, there have been recent advances in the ability to capture iris image at a distance. In current systems, however, the distance between the iris and the systems has to be less that 1 meter[684].

A common characteristic of the above mentioned examples is that many behavioural biometrics *do not have the discriminatory power to identify* an individual[685], at least not like traditional biometrics that aim for the highest possible uniqueness of the identifier. Some have argued that that behavioural biometrics are per nature *less discriminatory*, in the sense that they cannot reveal information on the identity of an individual. The potential to provide a broad categorical classification rather than full identification is invoked as a privacy enhancing quality behavioural biometrics may provide. However, on the other hand, they tend to *reveal more sensitive (and hidden) information about a person that could be used to categorise a subject into a group of people*.

The factors that are influencing the successful implementation of behavioural biometrics are mainly the same as first-generation (error rates, enrolment time, persistence, obtrusiveness). Most behavioural biometrics are, however, also very sensitive to the means of implementation, which may vary a lot according to different types of behavioural trait being collected. For instance, gait recognition techniques are quite sensitive to illumination changes, keystroke dynamics is sensitive to the keyboard hardware, and so on.

Within the wider category of second-generation biometrics, *soft biometrics* are also usually listed. Soft biometrics include very general traits like gender, height, weight, age and ethnicity, that lack the distinctiveness and permanence to sufficiently differentiate any two individuals and uniquely recognise a person (and for this reason they are called *soft*)[686], but are (a) easily measurable human characteristics, (b) can be obtained via cheap sensors and simple methods and (c) offer an added value to biometric systems by providing ancillary information. Although soft biometrics are weak characteristics and can be easily spoofed, they provide some evidence about the individual's identity that may be beneficial. For this reason, they are often used for performance improvement, to complement the identity information provided by the primary biometric identifiers and to improve the success rates of identification technolo-

[683] A survey on current iris recognition methodologies is available at Bowyer Kevin, Karen Hollingsworth and Patrick J. Flynn, "Image Understanding for Iris Biometrics: a survey", *Computer vision and Image Understanding*, Vol. 110, No. 2, 2008, pp. 281-307.
[684] De Marsico, Maria, Michele Nappi, Daniel Riccio and Harry Wechsler, "Iris segmentation using pupil location, linearization and limbus boundary reconstruction in ambient intelligent environments", *Journal of Ambient Intelligence and Human Computing*, No.2, 2011, pp. 153-162.
[685] Probably only two behavioural biometrics are believed to be useful not only for verification but also for reliable large scale identification, i.e signature/handwriting and speech. See Yampolskiy and Govindaraju, op. cit., 2008.
[686] See Jain, Anil K., Sarat Dass and Karthik Nandakumar, "Can soft biometric traits assist user recognition?", *Proceedings of SPIE Defence and Security Symposium*, Orlando Florida, 2004.

gies[687]. Soft biometrics are unable to individualise a subject, but they *can be very effective at distinguishing groups of people*.

TECHNOLOGY	STATE OF THE ART AND EMERGING TRENDS
Soft biometrics	Soft biometrics can either be continuous (such as height or weight) or discrete (such as gender, ethnicity). While they are not sufficient for identification or verification, they can be easily collected, they are effective for distinguishing groups of people, and can be combined with other biometric approaches to increase system accuracy.

As already mentioned, a new trend in biometrics of second-generation is the capture of biometrical traits *from a distance* or *on-the-move* for certain modalities, such as face recognition[688], iris recognition[689] and gait[690]. Biometric recognition of this type can work at a distance, usually without co-operation or explicit action required from the users. Examples include research on CCTV camera networks for security purposes[691], as well as projects targeted toward ambient intelligence[692]. However, biometric identification at-a-distance is still in the research domain[693] and not yet considered to be sufficiently mature for deployment[694]. The research on sensor technology at a distance has been identified as "a primary research challenge" by the US National Science and Technology Subcommittee in Biometrics 2006[695], while one year later the BioSecure network in Europe called research in distributed sensor networks and the "transparent use of biometrics requiring no actions from the end-users" one of the most urgent research topics in the field. From an engineering perspective it is often said that the flexible data acquisition protocol with the least amount of user cooperation is *improving user acceptability*. This class of biometrics is very well suited also to integrate identity

[687] See Jain Anil K., Sarat Dass and Karthik Nandakumar, "Soft biometric traits for personal recognition systems", *Proceedings of International Conference on biometrics authentication*, HK 731-738, 2004.
[688] The face is probably the most accessible and natural biometric trait at a distance. See Médioni, Gérard, Jongmoo Choi, Chang Hao Kuo and Douglas Fidaleo, "Identifying noncooperative subjects at a distance using face images and infrared three dimensional face models", *IEEE Trans Systems Man, Cybernetics – Part A: Systems and Humans*, Vol. 39, No. 1, 2009, pp. 12-24
[689] See Matey James, David Ackerman, James Bergen and Michael Tinker, "Iris recognition in less constrained environments", in N. K. Ratha and V. Govindaraju (eds.), *Advances in Biometric Sensors, Algorithms and Systems*, 2008, pp. 107-131.
[690] Nixon, Mark, Tienu Tan and Rama Chellappa, *Human Identification based on gait*, Springer Science + Business Media, New York, 2006.
[691] Such as the EU funded project PRISMATICA - see Velastin, S. A., L. Khoudour, B. P. L. Lo, J. Sun, and M. A. Vicencio-Silva, *Prismatica: a multi-sensorsurveillance system for public transport networks,* 2004. http://eprints.ucl.ac.uk/1355/1/2004_48.pdf and VITAB Network, "Video-based Threat Assessment and Biometrics Network". http://dircweb.king.ac.uk/vitab
[692] Such as smart beds that monitor the sleep patter, heart and breathing rate of seniors.
[693] For an overview, see Tistarelli, Massimo, Stan Z. Li and Rama Chellappa, *Handbook of remote biometrics for surveillance and security,* Advances in Pattern Recognition Series, Springer-Verlag, London, 2009
[694] See *Biometric technology Today, "*Iris at a distance not yet mature enough, says UAE", Vol. 17, No. 2, Feb. 2009, p. 1.
[695] National Science and Technology Council, SubCommittee on Biometrics, *The National Biometric Challenge*, August 2006.

recognition and surveillance tasks, but can give rise to important concerns on covert data capture, transparency and user's consent.

While first generation biometric systems typically deploy a single modality even for large scale applications, second-generation biometrics, which are often less robust than conventional biometrics, must consult more modalities at a time. *Multimodal systems*, which take into account several different biometrics in a simultaneous way, are rapidly progressing[696]. These consist of different types of biometrics used in combination and can be a good way of adjusting the security/convenience trade off in a biometric system. Multimodal systems are generally applied to reduce the false acceptance rate and improve the recognition performance of a system, or to facilitate the data acquisition for a wider population. In multi-modal biometrics, each modality is expected to effectively corroborate the other. However, the main drawbacks of these systems are the high costs for their use and the fact that the complexity and time for the enrolment/verification processes are higher than for uni-modal systems[697]. Multimodal systems can be implemented by authenticating a user on a number of multiple modalities at the same time (parallel scheme) or in a cascade (serial scheme). Depending on traits, sensors, and features used, there are four major categories of multimodal biometric systems: 1) single biometric trait, multiple sensors; 2) single biometric trait, single sensor, multiple classifiers; 3) single biometric trait, multiple sensors and units; 4) multiple biometric traits, multiple sensors. The main disadvantages of multi-modal systems are that they have high financial costs and potentially necessitate a larger user involvement and a more consistent amount of data being captured.

Finally, there are additional emerging techniques that aim to support the security of a biometric system against attacks or tentative frauds. The *aliveness detection module* is a particularly well-researched methodology, although its effectiveness has yet to be fully established. Aliveness detection modalities can detect a person's physiological sign of life, in order to avoid being cheated by artificial (fake) attributes. It has also the potential to generate extra data, as it aims at testing some physiological responses that can generate unintended information about medical conditions or emotional states.

5.3 DRIVERS AND BARRIERS TO SECOND-GENERATION BIOMETRICS

According to the US National Science & Technology Council – Subcommittee in Biometrics 2006 paper on *The National Biometrics Challenge*, "the future of the biometrics community will be shaped by four primary driving forces"[698]: (i) national security, (ii) homeland security and law enforcement, (iii) enterprise and e-government services, (iv) personal information and business transactions. The report also lists four preeminent challenges for the biometric community: to improve collection devices (biometric sensors), to develop more efficient and effective large scale operational capabilities (biometric systems), to establish standards for

[696] A notable example is the US VISIT program, that exploits face and fingerprint data.
[697] A proposed solution to overcome these drawbacks could be the incorporation of intelligent agents into multimodal biometric systems. An agent-based adaptive biometric system may choose among different modalities and modes of interaction according to the situation. See Deravi, Farzin, Michael Fairhurst, R Guest, Nick Mavity and Anne Canuto, "Intelligent Agents for the Management of Complexity in Multimodal Biometrics", *International Journal of Universal Access in the Information Society*, Vol. 2, No. 4, 2003, pp. 239-304.
[698] National Science & Technology Council, Subcommittee in Biometrics, *The National Biometrics Challenge*, 2006.

plug and play performance (biometric interoperability) and to enable informed debate on why, how and when biometrics should be used (biometrics communication and privacy).

Biometric systems are increasingly used both by governments and private companies in very diverse settings. The public sector, comprising law enforcement and transport markets, is the main user segment of the global biometric market. Banking, financial and healthcare sectors are expected to grow over the next ten years. Biometrics are also likely to be increasingly introduced in education, retail, telecom and corporate enterprises. According to a 2009 market research forecast, the biometric global market is expected to experience significant growth in the current decade.[699] From a geographical perspective, North America and Europe currently enjoy dominance in the market, but the Asia-Pacific region is expected to generate the greatest per cent of global revenues (32%) for the biometric industry by 2017[700]. With respect to the technologies being developed, the dominance of AFIS and fingerprint-based identification will continue, but by the end of the next decade iris and face recognition will increase their share and account together a third of the market.

With particular reference to the "second-generation biometrics" market, a recently published market research report pointed out that the current decade is also expected to be marked by the "fusion of CCTVs with biometrics (face recognition) and human behaviour signatures" [701]. According to the report, the fusion of CCTV with biometrics can be a solution for the cost of security officials in high security applications, for instance, supporting the potential to providing a real time alarm when a suspect is viewed by a camera. This new market is forecasted to reach $3.2 billion by 2016 and will mainly rely on particular technological segments, identified by the report as "walk-in systems, remote biometric identification systems, passive remote behaviour detection and tracking systems, stimuli triggered remote behavioural surveillance".[702]

Scholars agree that we are witnessing a significant change in the deployment of biometrics. If large scale identification schemes of the past relied on secure ways of identifying individuals, some interesting trends are creating an *ever-increasing interest in behavioural biometrics for soft recognition purposes*[703]. The first trend is related to security applications, and refers to the fact that most of the terroristic attacks of the past have been committed by previously unknown people. This implies that the focus needs to be put more on the *detection of a suspicious behaviour rather than on the true identity of a person*. The second trend concerns the development of Ambient Intelligence, which implies *a technology that automatically recognises specific needs of people through observation of behaviour*. In the digital age, behavioural biometrics and related technologies have the potential to improve diverse areas, such as

[699] Most, Maxine, *The future of biometrics: Market Analysis, Segmentation and Forecast*, ACUITY Market Intelligence Report, 2009. http://www.acuity-mi.com/FOB_Report.php

[700] Scholars have pointed out that clear differences emerge among different countries approaches to biometrics: while in the West biometrics are mainly associated with security issues, in some Asian countries such as Japan and Singapore, their commercial uses are as important as security applications. See Mc Carthy, Paul, "Biometric Technologies, Ethical Implications", in Dan Callaghan Peter Singer, Ruth Chadwick (eds.), *Encyclopedia of Applied Ethics*, 2nd Edition, Academic Press, London, 2011.

[701] Homeland Security Market Research, *CCTV based remote biometric and behavioural suspect detection: technologies and global markets – 2011-2016*, Washington DC, 2011. http://www.homelandsecurityresearch.com/2011/02/cctv-based-remote-biometric-behavioral-suspect-detection-market-2011-2016

[702] *Ibid*

[703] See Schumacher, Gunther, "Behavioural biometrics: emerging trends and ethical risks", to appear in Mordini and Tzovaras, op. cit., in press.

e-commerce and other personalised services. The third trend is profiling, the *combination of many different pieces of personal information for commercial (e.g. behavioural advertising), or security purposes*. From an engineering perspective, and having taken into account these new trends, behavioural biometrics provide an additional advantage over traditional biometrics, in that they can be collected less obtrusively, sometimes even without the knowledge of the individual. However, as will be discussed below this raises crucial privacy and ethical issues about transparency and consent.

In conclusion, the main drivers of today's development and deployment of the "next generation" of biometrics include:

- advances in sensor technologies that enable different bodily behaviour characteristics to be captured, and the emergence of potentially new biometric traits
- added value offered by soft biometrics, used for any kind of recognition to improve the system performance or for automated categorisation of individuals
- use of multiple biometrics or multimodal systems to improve the system accuracy
- decreased intrusiveness of systems through the remote capture of data
- cost-effectiveness of the collection of behavioural data that does not require any special hardware[704]
- advances in technologies to ensure security and privacy: template protection, encryption, aliveness detection, anti-spoofing are becoming an essential component of any biometric system
- inclusion of biometric in the "software as a service" and cloud computing emerging trends[705]

The main barriers include:

- behavioural biometrics are not strong enough to compete with first-generation biometrics for primary identification, since they rely on weaker (i.e. with low discriminatory content) and less persistent body traits
- more (e.g. multimodal systems) and more sensitive information (sensitive personal data, medical information) can be revealed
- covert data capture raises concerns on consent and transparency
- interoperability and standardisation are not yet mature aspects of these technology

5.4 APPLICATIONS

Due to technological advances and increased demands for security as well as human cost-saving and operational efficiency reasons, recent years have seen significant increase in the deployment of biometric recognition systems. Despite the abundance of biometric sensing devices and algorithms, not all of them are equally suited for all applications. Their suitability mainly depends upon the reliability of the system, a low enrolment and training time and a resistance to spoofing. This is mainly true for traditional biometrics deployed in large scale identification systems. On the other hand, profiling and surveillance applications as well as ambient intelligence applications require a high degree of unobtrusiveness that can be better-provided by second-generation biometrics. From an operational perspective, the identification

[704] This is however not true for all biometrics of second-generation. Some behavioural biometrics require specialised and highly intrusive equipment, while others can offer a completely unobtrusive and easy way to classify individuals.

[705] An example is the possibility that the e-passport infrastructure will migrate to the cloud. See "Demand for Mobile and Cloud-Based Credentials Growing According to Entrust Presentation at International Civil Aviation Organization Symposium", Find Biometrics, Sept 2011. http://www.findbiometrics.com/industry-news/i/9247 and this paper.

accuracy of next-generation biometrics may not be adequate to meet the requirements of high security or large scale applications, but they can be used where *strong identification is not a necessary condition*, such as some online authentication schemes or in a user-centred intelligent environment.

In this section we will focus on traditional applications of biometrics and on current research projects on next-generation biometrics. Many second-generation biometrics are not considered a mature technology for deployment. Their weak robustness and their propensity to change over time means that very few systems based on these traits have been deployed so far. However, some emerging trends are visible, which give some indication of future opportunities, challenges and potential risks.

5.4.1 Traditional biometrics

Until recently, nearly all major applications of biometrics have been government-led and concerned with national security and law enforcement (security applications), or with operational efficiency in national ID and social welfare programs (e-government, e-Health). Large scale public sector biometric usage currently represents 70% of the world biometric market[706]. Such large scale applications, based on robust and highly distinctive biometric identifiers, expect high accuracy and throughput under varying operating conditions, rapid collection of biometric data with virtually no failure to enrol and low FAR, high levels of privacy and template protection.

Traditional biometrics were first used in security applications such as law enforcement, surveillance and border control procedures. Primary forensic and law enforcement applications currently include the IAFIS system of the FBI[707], DHS IDENT system[708], the UK national criminal intelligence DNA database[709]. With reference to surveillance purposes, China has recently started a national network of surveillance cameras, biometric identification cards, and facial recognition software with the "Safe City Safety Surveillance Ordinances bill", requiring the 660 country's largest cities to install surveillance systems in major public venues, such as subways and municipal buildings. The Chinese government also used biometrics technologies with face recognition for the opening and closing ceremonies in the 2008 Beijing Olympics. European authorities have also experimented with the use of biometrics in programmes designed to curb hooliganism. EU institutions' wide investment in various border security and control initiatives has made the EU one of the single largest biometric markets in the world. Major examples of traditional biometrics in border control procedures include biometrics used

---

[706] See BCC Research, "Biometrics: Technologies and Global Markets". http://www.bccresearch.com/report/biometrics-technologies-markets-ift042c.html

[707] Integrated Automated Fingerprint Identification System (IAFIS, more information available at FBI website, IAFIS webpage, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis). The FBI has recently announced the plan to have a multi-modal database (allowing the collection of fingerprints, palm prints, iris scan, but also voice data, that is designed to expand to include other biometric identifiers in the future - see the Electronic Frontiers Foundation, "FBI next generation identification database", 2011. https://www.eff.org/deeplinks/2011/07/fbis-next-generation-identification-database

[708] Automated Biometric Identification System. A privacy impact assessment on IDENT is available: Department of Homeland Security, IDENT PIA, 2011. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf. More information on IAFIS / IDENT interoperabilità can be found at Department of Homeland Security, US IAFIS-IDENT Report, 2001. http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_IDENT-IAFISReport.pdf

[709] The so called NDNAD was set up in 1995 and for many years was the world's largest forensic DNA database. More info at the UK Police, "NDNAD", 2011. http://www.npia.police.uk/en/8934.htm

at international border crossing points such as the US-VISIT program[710], and the EU VIS[711], SIS[712] or EURODAC[713] systems in Europe[714], as well as the deployment o biometric technologies at airports, such as face recognition at Sydney and Melbourne airports[715], iris recognition at Schiphol[716] and Frankfurt, fingerprint in Japan[717] and Hong Kong[718]. It is reasonable to expect that in short time all personal documents will contain some form of biometric data.

Biometrics have also been used in national ID and social welfare programs. The Indian government has recently announced a new project called Unique ID[719] to deliver a biometric-based national ID card to over a billion of citizens. It is the biggest identification project ever put in place and is expected to create the largest biometric database on the planet. The Unique ID project could become a model of very large scale usage of biometrics in e-governance, and Indian authorities expect it to be an important tool for the inclusion of millions of people into governmental social welfare programs, as well as a tool to fight criminality and terrorism. In the past decades, Europe has seen a lot of investment in biometrics by state and private companies in various e-governance, access control/time attendance and network security initiatives. Netherlands' Ministry of Justice has deployed fingerprint-based biometrics to activate user authentication, provide digital signatures, support encryption of data and documents, and enhance email security. The National Identity Scheme UK (*Ident1*) was initiated by UK gov-

[710] See DHS, "US Visit Program", 2011. http://www.dhs.gov/files/programs/usv.shtm

[711] Visa Information System (VIS). The European Union Visa Information System (VIS) is a database containing information, including biometrics, on visa applications by Third Country Nationals requiring a visa to enter the Schengen area. This biometric information (10 fingerprints and a facial image), in VIS will remain valid for five years. Information is centrally stored in a database in Strasbourg (with a back-up site in Austria) allowing checks to be made at border crossing points that the person holding the biometric visa is the person who applied for it. This database is expected to contain some 70 million biometric records at full capacity. VIS aims to prevent visa fraud and visa shopping by applicants between EU member states and to facilitate checks at external border crossing points and within territory of member states, assisting in the identification of listed persons. The bodies having access to VIS include Consulates and police authorities from member states and Europol.

[712] Schengen Information System (SIS and SIS II). SIS is a governmental database used by several European countries to maintain and distribute information on individuals and pieces of property of interest. The intended uses of this system is for national security, border control and law enforcement purposes. Information in the SIS is shared among institutions of the participating countries in the Schengen Agreement Application Convention (SAAC). SIS II is the advanced version of the Schengen information System

[713] EURODAC is a large database consisting fingerprints of asylum and illegal immigrants within the EU. Asylum applicants and irregular border-crossers over the age of 14 have their fingerprints taken as a matter of European Community law. These fingerprints are then sent in digitally to a central unit at the European Commission, and automatically checked against other prints on the database. Currently, The European Data Protection Supervisor (EDPS) supervises the processing of personal data in the database (central unit) and their transmission to the Member States.

[714] See EUROPA website, "Legislation Summaries: Free movements of persons, asylum and immigration", 2011.
http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration

[715] See Australian Government – Department of Immigration and Citizenship, "Smart gate automated border processing", 2011. http://www.immi.gov.au/media/fact-sheets/71smartgate.htm

[716] See Schiphol Airport, "Fast Border Passage with the iris scan", 2011.
http://www.schiphol.nl/Travellers/AtSchiphol/PriviumIrisscan/WhyPrivium/FastBorderPassageWithTheIrisScan.htm

[717] See Tokyo Topia, "Tokyo Narita Landing Procedures", 2011. http://www.tokyotopia.com/tokyo-narita-landing-procedures.html

[718] See CEM System, "Hong Kong International Airport Project", 2011. http://ftp.cemsys.com/download/Project_Profile_Hong_Kong_International_Airport.pdf

[719] See Government of India, "Unique Id Project", 2011. http://uidai.gov.in

ernment to help citizens access to public services, employment, stop illegal immigration and working, and tackle crime and prevent terrorism[720].

Advances in technologies and the widespread availability of biometrics have also spun out an ever-increasing number of private applications beyond national security or governmental operational efficiency concerns. The financial and healthcare services sectors are rapidly adopting biometric technologies to secure physical and logical access. Biometrics are also increasingly used in business applications, such as worker time registrations. In the relatively near future, biometrics can be expected to gain increased acceptance in all kinds of access and attendance control applications. The national authorities in charge of data protection are playing a prominent role in authorising the use of biometrics in such situations.

5.4.2 Future biometrics: surveillance and ambient intelligence applications

Because second-generation biometrics still in the research domain, it is not possible to describe current applications as we have for traditional biometrics, or to comprehensively explore the long term consequences of their deployment. Behavioural biometrics are, however, increasingly being considered for security and non-security purposes.

Some authors have said that currently deployed biometric systems represent only "a limited portion of the real potential of biometric technologies"[721]. Unlike traditional biometrics that rely on more persistent, robust and distinctive body traits, next-generation biometrics are not expected to be adequate to meet the large scale security applications requirements of the public sector alone; they could, however, play an important role as a tool to support surveillance and profiling applications. Biometric systems are also expected to be used for personal security and convenience in home automation, retail, gaming and other intelligent environment applications. According to this view, biometric technologies could be more intensively exploited, particularly in the wider domain of man-machine interaction, where relevant information may not be the one that *identifies* an individual but that *characterises* him or her. Biometrics could represent an important, facilitating element in the trend towards ambient intelligence and ubiquitous computing, given the potential for continuous, autonomous, real-time, unobtrusive authentication. Second-generation biometrics can greatly ameliorate the interaction between the user and an *intelligent* environment.

While many behavioural biometrics are still in their infancy, some very promising research has already been done. Some examples of recently-funded EU research initiatives in these fields include the research projects that are indicated below.

Projects on biometrics for authentication and identification for Ambient Intelligence:

- the HUMABIO project (Human monitoring and authentication using biodynamic indicators and behavioural analysis)[722] which has proposed a posture analysis authentication mechanisms for preventing the hijacking of heavy good vehicles;
- the ACTIBIO project (Unobtrusive authentication using activity related and soft biometrics)[723] which aims at developing methods for ongoing authentication based on

[720] The Ident1 card scheme was eventually scraped by the Identity documents Act in 2010.
[721] Tistarelli, Massimo, and Ben Shouten, "Biometrics in Ambient Intelligence", *Journal of Ambient Intelligence and Human Computing*, Vol. 2, 2011, pp. 113-126.
[722] HUMABIO project, 2011. http://www.humabio-eu.org
[723] ACTIBIO project, 2011. http://www.actibio.eu:8080/actibio

users' response to specific events and being fully integrated in ambient intelligence infrastructures;
- the AMIGO project (Ambient Intelligence for the networked home environment) aims at developing "open, standardized, interoperable middleware and attractive user services" for ambient intelligence at home[724];
- the MOBIO project (Mobile Biometry)[725] which aims to develop new mobile services secured by biometric authentication means.

Projects on the use of camera networks for security purposes:
- the PRISMATICA project (Proactive Integrated systems for Security Management by Technological, Institutional and Communication Assistance)[726], which aims to explore new CCTV technological solutions to be exploited for the enhancement of security management in the public transport sector;
- the VITAB network (Video-based Threat Assessment and Biometrics Network)[727] with the main aim of improving the effectiveness of CCTV control room operations to support surveillance in town centers, public transport and sensitive sites

Projects focusing on the recognition of behaviours or actions of a subject or group of subjects:
- the CAVIAR project (Context Aware Vision using Image-based recognition)[728] aimed at exploring new mage-based recognition technologies potential applications for city center and commercial surveillance;
- the SAMURAI project (Suspicious and abnormal behaviour monitoring using network cameras for situation awareness enhancement) with the objective to "develop and integrate an innovative intelligent surveillance system for monitoring people and vehicle activities at both inside and surrounding areas of a critical public infrastructure".[729]
- the ADABTS project (Automatic Detection of Abnormal Behavior and Threats in crowded Spaces) aims at developing a real time platform "for high performance and low cost surveillance systems".[730]

In the US, public attention has recently being captured by a project funded by the Department of Homeland Security under the acronym of FAST (Future Attribute Screening Technology) that aims "to detect *malintent*" prior to its execution by screening people for "psychological and physiological indicators"[731], i.e. through the combination of body signal and motor skills biometrics.

5.4.3 Online and on-the-cloud biometrics

An emerging trend is the increase of interactions between the real and virtual world. The Internet is becoming a more pervasive part of our daily lives. The management of particular online identities that could be used for different purposes is an area of particular interest. Em-

[724] AMIGO project, 2011. http://www.hitech-projects.com/euprojects/amigo
[725] MOBIO project, 2011. http://www.mobioproject.org
[726] See Velastin, op. cit., 2004.
[727] VITAB network, 2011. http://dircweb.king.ac.uk/vitab
[728] CAVIAR project, , 2011. http://homepages.inf.ed.ac.uk/rbf/CAVIAR
[729] SAMURAI project, 2011. http://www.samurai-eu.org
[730] CORDIS, "ADABTS project", 2011.
http://ftp.cordis.europa.eu/pub/fp7/security/docs/adabts_en.pdf
[731] DHS, "Human Factors/Behavioural Science Projects", 2011.
http://www.dhs.gov/files/programs/gc_1218480185439.shtm#6

erging trends include the need to certify identities for online financial transactions, as well as more controversial applications based on tracking users' online behaviours for personalised advertising. Biometrics are likely to be increasingly incorporated as an identity verification method in different online transactions. If biometric technologies are at an early stage of their commercial development, their transition into the virtual environment may deeply impact on their wider deployment. Research is currently underway to explore potential uses of biometrics in the online environment.

However, the huge potential for sharing biometric data over the Internet has to be taken into account and the legal and social implications urgently need to be addressed. The latest controversy between Facebook and some privacy advocates in the US and data protection authorities in Europe may give some clues of the emerging non-technical implications. In December 2010, Facebook announced plans[732] to implement a facial recognition tool intended to make it easier for people to tag photos of other persons. Facebook "tag suggestion feature" uses facial recognition software[733] that matches the uploaded photo to other – already tagged – photos and suggests a person to be tagged[734]. Much of the controversy surrounding Facebook's facial recognition feature comes from the fact that, when it is initially implemented, it is turned on by default instead of allowing users to opt in. A Facebook user must update his or her privacy settings to opt out of the feature. The company huge database of users' personal data had raised critical concerns. In the US, in June 2011, the Electronic Privacy Information Center (EPIC) sent a complaint[735] to the Federal Trade Commission (FTC), urging the FTC to examine Facebook's implementation of facial-recognition technology. In August 2011, the Hamburg Data Protection authority sent a letter to Facebook requiring it to disable the software and delete any previously stored data. According to the German DP Authority, the social network website is creating the world's largest database of biometric information: users have uploaded an estimated 75 billion photos to the social-networking site and 450 million people have been tagged. This claim has been recently rejected by Facebook[736]. The EU's Article 29 Data Protection Working Party, and other national data protection authorities, are also investigating any potential privacy violations and will advise national authorities in Europe.

Another interesting trend is the potential for biometrics to be incorporated in cloud computing infrastructures. For example, a provider of online identity and IT security solutions has recently reported giving a talk on the evolution of its e-passport technologies and on the growing interest in cloud services[737]. Migrating the e-passport infrastructure on the cloud could be effective in terms of cost-savings and achieving uniform standards in that field, however it raises even more severe concerns over the security of the biometric templates and privacy and

[732] Through a blog post (available at https://blog.facebook.com/blog.php?post=467145887130) According to this post, over 100 million tags are added to photos by users every day.

[733] The system examines the newly uploaded photos and compares them to other photos in which an individual is tagged in order to make tagging suggestions. The face recognition software used by Facebook, Phototagger, has apparently been produced by the company Face.com, see Perez, Sarah, "Photo tagger: Facial recognition for auto-tagging Facebook photos", ReadWriteWeb, 21 July 2009. http://www.readwriteweb.com/archives/photo_tagger_facial_recognition_for_auto-tagging_facebook_photos.php

[734] This allows a "one-click" tag procedure, instead of typing the name of the tagged person.

[735] EPIC, "Facebook Privacy", 2011. http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf

[736] Fiveash, Kelly, "Facebook facial recognition tech violates German privacy laws", *The Register*, August 2011. http://www.theregister.co.uk/2011/08/04/germany_no_to_facebook_facial_recognition

[737] The provider is Entrust, and the talk was given in occasion of the ICAO 7th Symposium in Montreal, September 2011. See http://www.findbiometrics.com/industry-news/i/9247 Entrust technology is currently in use in many countries, including the US, UK, Taiwan, Singapore, Ireland, Canada, New Zealand, Finland

protection of personal data – with evident implications for the individual participation principle in accessing their personal data that are processed by a (potentially unknown) third party.

5.5 PRIVACY IMPACTS AND ETHICAL ISSUES OF SECOND-GENERATION BIOMETRICS

In parallel with their wider deployment, biometrics are acknowledged to have the potential to raise critical ethical, social and legal concerns, which can impact social acceptability of biometric identification methods. While scientific literature on the societal aspects of traditional biometrics has seen great increment in the last decades, the specific ethical and legal implications for second-generation biometrics still need to be properly addressed. Most general concerns raised by traditional biometrics are related to the protection of individuals' values, such as privacy, autonomy, body integrity dignity and personal liberty. The most critical implications of next-generation biometrics mainly refer to the fact that biometric recognition could take place covertly (remote, from a distance) and may produce material with a high degree of surplus (and sensitive) information. Many of the motor-skill based biometrics may reveal a physical handicap of a person and result in potential discrimination. Other biometrics can reveal emotional states or other information that could be perceived as highly intimate by the individual. In this section we will address crucial ethical and legal concerns raised by biometrics, trying to remark the differences between biometrics of first- and second-generation. However, the implications addressed in the following sections are to be considered as very general remarks and biometric technologies and applications must be differentiated.

5.5.1 Human dignity and the informatisation of the body

One of the main philosophical concerns raised by this technology relates to the fact that biometrics are strictly linked to the human body, whose integrity (physical and psychological) constitutes a key element of human dignity that is protected in the main international legal instruments as a fundamental human right – and moreover, represents the basis for the protection of other human rights. The human body, as the result of the integration of the physical body and the mind, has a strong symbolic dimension, as it lies at the heart of our essence. Practices involving the human body are "unavoidably invested with cultural values and in their turn produce new values"[738].

The human body can be "measured" for different purposes, such as for medical monitoring in order to identify pathological conditions. It can be also measured to ascribe people to different categories or identify individuals. The legitimacy for biometrics as a tool for *identifying* individuals has been discussed in depth[739]. In particular, the French Ethical National Council raised severe doubts about the legitimacy of using biological features – instead of biographical – to identify individuals[740]. In its 2008 opinion, the French Authority warned against the potential for the widespread use of biometrics to *instrumentalising* the human body, and to reducing the human person to an accumulation of digital (and simplified) data. The opinion also mentioned the growing use of "behavioral features" not only to *describe* an individual, but also to *define* who he is and what he does/consumes (page 4).

[738] Mordini, Emilio, *Whole Body Imaging at airport checkpoints: the ethical and political context*, HIDE&RISE policy report, February 2010 (updated March 2011). www.riseproject.eu

[739] Mordini, Emilio, and Sonia Massari, "Body, Biometrics and Identity", *Bioethics*, Vol. 22, No. 9, 2008, pp. 488–498. http://www.hideproject.org/downloads/Mordini_Massari-Body_Biometrics_Identity.pdf

[740] National Consultative Ethics Committee for Health and Life Sciences, *Biometrics, Identifying Data and Human Rights*, Opinion No. 98, 20 June 2008.

In line with this view, scholars speak of an "*informatization* of the body" with reference to the digitalisation of physical and behavioural attributes of a person and their distribution across the global information network[741]. At the core of this concept there is a concern for the simplification of human attributes through digitalisation that could affect representations of ourselves, and may produce processes of *disembodiment* or body dehumanisation, or offend human dignity[742]. Some scholars refer to the development of soft, behavioural, electrophysiological biometrics (the so called "*under the skin biometrics*"), as well as to the potential for distant and covert data capture, as a further step in the informatisation of the body. This is mainly based on the idea that these systems represent "a significant increase in the extent to which bodies are assumed to become available"[743]. Although the informatisation of the body is a relatively new phenomenon, it is evident that critical attention should be paid to today's exponential growth in the *amount* and *quality* of bodily data available with improved biometric technologies.

5.5.2 Function creep

Function creep relates to the concept of a technology that was designed for one purpose being used for a completely different purpose. It can be driven by technological innovation or by missing policy parameters. In the field of automated personal recognition, function creep may be motivated by several reasons, from state intelligence and crime control, to commercial purposes. It usually involves three elements: 1) a policy vacuum; 2) an unsatisfied demand for a given function; 3) a slippery slope effect, or a covert application[744].

In the field of biometrics, the best known example of function creep is EURODAC, established to enhance the common asylum policy and then opened up to police and other law enforcement agencies. However, there are many national large scale centralised database that are posing the same risk. Once the database is established, there is always a potential for it to be used for future applications that may differ from its original purpose. It is also difficult for a government to provide assurances in relation to this issue, unless a technological solution is put in place to specifically avoid function creep.

Behavioural biometrics are likely to strengthen the potential for function creep, because of the very sensitive nature of the data collected and the possibility to use such biometric data, if centrally stored, to carry out data mining research, which could be targeted to specific groups of people. The collection of ancillary and particularly sensitive information of second-generation biometrics can result in a more critical possibility for function creep, that may be facilitated by a surplus of information that behavioural and soft biometrics, as well as multimodal systems, are expected to produce. The purpose specification principle, that is among the main principles of the international data protection legislation, plays a key role in this respect, as it prescribes that biometric data should be collected only for *specified*, *explicit*, and *legitimate* purposes.

---

[741] van der Ploeg, Irma, *The Machine Readable Body. Essays on biometrics and the Informatization of the body*, Shaker, Germany, 2005.
[742] Mordini Emilio, "Ethics and Policy of biometrics", in Massimo Tistarelli, Stan Z. Li and Rama Chellappa (eds.), *Handbook of Remote Biometrics: For surveillance and Security*, Springer, Dordrecht, 2009.
[743] van der Ploeg Irma, "Security in the danger zone: normative issues of next generation biometrics", in Mordini and Tzovaras, op. cit. in press.
[744] Mordini and Massari, op. cit, 2008.

5.5.3 Privacy and data protection concerns

In PRESCIENT D1, privacy and data protection are described as different but intertwined concepts that have been long discussed from diverse perspectives. The protection of both principles is guaranteed by major international human rights legal instruments via the right to respect for private life and the right to the protection of personal data. The contemporary notion of *privacy* is "associated with the concept of autonomy, as the capacity to put distance between us and others, to develop our beliefs and desires, to maintain a certain level of control over the inner spheres of the self, to exercise a certain degree of individual power to make choices, to limit access to oneself and to be separate from the community"[745]. As individuals, we exist to the extent that we are able to make decisions and represent ourselves as autonomous beings. The individual power to be autonomous is, however, the result of the delicate balance between our desire to be independent and our need of the community.

Apart from the potential for biometrics to impact on *individual physical privacy* (see section 5.1), there is also the potential for biometrics to impact upon *individual autonomy and self-determination* more generally. Biometrics, and above all, behavioural and soft biometrics, may collect very sensitive information revealing medical status, racial origin, or other genetic information, and this poses serious concerns over the potential for discrimination of individuals in terms, for instance, of job opportunities, insurance coverage, and public recognition.

With reference to data protection implications of biometrics, biometric data are personal data[746] and as such they have to be processed, in Europe, under the scope of the EU personal data legislation[747]. The European legal framework for personal data protection[748] is based on principles such as purpose specification (as mentioned above), proportionality, confidentiality and individual consent and participation.

First, according to the EU Data Protection Directive, personal data should always be processed with the user's informed consent. With reference to the *individual participation principle*, identification procedures pose a much greater risk from a data protection perspective when personal data are stored in centralised databases and cannot be under the strict and full control of the individual. Covert techniques offer the potential to identify people outside the scope of the systems. Some behavioural biometrics can be collected without the user's knowledge: embedded technologies and remote and covert biometrics raise serious concerns on the free consent, transparency and on individual control over her personal data.

Second, biometrics have the potential to collect *extra information*, and this is especially true for behavioural biometrics, which could detect people's emotional states, or information about their medical history, as well as for multimodal systems, in which many modalities are combined. These practices may deeply impact on the *proportionality* principle.

[745] PRESCIENT project Deliverable 1, page 21.
[746] On the controversial definition of biometric as personal data see chapter 6 on "Extent to which the existing legal frame work addresses the privacy and data protection impacts".
[747] De Hert, Paul, Scheurs Wim and Brouwer Eveline, "Machine readable identity documents with biometrics data in the EU – part III – Overview of the legal framework", *Keesing Journal of Documents and Identity,* Vol. 22, 2007, pp. 23-26.
[748] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

Finally, Art. 8 of the EU Data protection Directive states a general prohibition of processing of sensitive data. The degree of *sensitivity* of biometric data varies according to the kind of biometric features (physical or behavioural), the modality (unimodal vs. multimodal) and the storage format (row image vs. template). It is often said that the deeper biometric technologies look into the human body, the more they might reveal particular sensitive information[749]. According to the Art. 29 WP 2003 working document on biometrics, "some biometric data could be considered as sensitive in the meaning of Article 8 of Directive 95/46/EC and in particular, data revealing racial or ethnic origin or data concerning health", that is exactly the kind of information that some soft and behavioural biometrics might provide.[750]

5.5.4 Profiling and surveillance

As already mentioned, the sensitivity of some information revealed by the processing of behavioural biometrics may raise deep concerns over the potential for function creep, when the collected data is used for secondary purposes. Function creep is even more likely to happen for second-generation biometrics, which are focused on more intricate behavioural characteristics of the human body, on states or emotional conditions, even though next-generation biometrics seek to generate only "partial identities" of an individual, to ascribe him or her into specific categories.

Profiling refers to an automatic data processing technique that consists of applying a profile to an individual, particularly in order to take automatic decisions concerning him or her for analysing or predicting her or his personal preferences, behaviours or attitudes. Profiles can be used to classify or even to track individuals. Profiling is a key area of concern for next-generation biometrics. Even if they are linked to less distinctive and persistent body traits, physiological states or habits may reveal more sensitive information than traditional biometrics. This sensitive information can be better exploited for targeted surveillance and profiling purposes. However, this can only become a realistic scenario when it will become technologically possible to mine and link vast amounts of sensors and data.

The FIDIS report has performed a comprehensive analysis of the profiling aspects of behavioural biometrics[751]. The major risks the report identified include discrimination (information used to exclude persons from certain areas), stigmatisation (risk of longer term profiles with negative interpretation), "unwanted confrontation" (with, as an example, information on the health status, in the case that body signals indicate certain diseases for which the medical treatment is unlikely or even impossible).

5.5.5 Social inclusion/exclusion, risk of stigmatisation, discrimination, digital divide

The introduction of soft and behavioural biometrics has raised serious objections on the basis that it could constitute or facilitate discriminatory social profiling. Discriminatory practices might be perpetuated on a non-voluntary basis. As an example, as a more and more use of

[749] A recent study revealed that EEG patterns may be used to extract "significant information about the thoughts of the subject from records of brain activity (fMRI)". See Naselaris, Thomas, Ryan J. Prenger, Kendrick N. Kay, Michael Oliver and Jack L. Gallan, "Bayesian Reconstruction of Natural Images from Human Brain Activity", *Neuron*, Vol. 63, No. 6**,** 2009. http://www.cell.com/neuron/abstract/S0896-6273(09)00685-0

[750] Article 29 Data Protection Working Party, Working Document on Biometrics, 2003.

[751] See FIDIS, "Deliverable D 7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools", 2009. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-biometric_profiling_and_transparency_enhancing_tools.pdf

biometrics is made, there can be an increasingly presumption that everyone should be able to enrol into a biometric system. However, the enrolment of injured and disabled groups[752] could lead to more false rejection rates than average. Ageing is a particular issue for most biometric modalities, but also children may have particular problems in being enrolled (mainly because they are still developing). Discrimination of this type happens involuntarily, but may deeply affect vulnerable individuals and impact on the principle of *equity*. Moreover, the issue of informed consent could be very critical for incapacitated and disabled persons. On the other side of the coin, biometrics can also provide practical support for the identification of groups of people who are not able to identify themselves in other ways.

The development of a biometric system may also produce discriminatory effects. As an example, a recent study[753] demonstrated that the geographic origin of an algorithm (where it was developed) affect how well it performs on faces of different races. This provides evidence about the presence of an "other-race effect" also in automated face recognition, as happens for human face recognition.

Finally, some biometric characteristics have the potential for direct disclosure of personal medical information, even if this may vary depending on the technologies used[754]. Relevant examples include:

- pictures of retina/iris that can reveal health status (diabetes), as well as lifestyle habits (drug use)
- gait recognition may reveal some muscle-skeletal disorders but also emotional states such as depression[755]
- voice recordings can reveal laryngitis or throat cancer
- Human-Computing Interface biometrics can reveal psychiatric and neurological conditions
- EEG, ECG, vein recognition may reveal hypertension or vascular abnormalities
- some sensors could detect surgical modification of the body

5.6 EXTENT TO WHICH THE EXISTING LEGAL FRAMEWORK ADDRESSES THE PRIVACY AND DATA PROTECTION IMPACTS

Since December 2009, the EU is operating on the basis of a legally binding bill of rights, while the current EU data protection framework was established before the Lisbon Treaty entered into force. Emerging technologies are raising new concerns over fundamental human rights that are leading to calls of modernisation of the EU data protection legal framework.

---

[752] Wickins has recently explored the vulnerability of a typical user population falling into six groups, mainly including people with physical or learning disabilities (e.g. spelling problems, walking impairments), people of certain races and religions, those that are elderly or homeless. See Wickins, Jeremy "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification", *Science and Engineering Ethics*, Vol. 13, 2004, pp. 45-54.

[753] See Furl, Nicholas, Jonhathan Phillips and Alice O 'Toole, "Face recognition algorithms and the other-race effect", *Cognitive Science,* Vol. 26 No. 6, 2002, pp. 797-815.

[754] Mordini, Emilio and Holly Ashton, "The Potential for Disclosure of Personal Medical Information", in Mordini and Tzovaras D., op. cit, in press.

[755] See Lemke, Mathias R, Thomas Wendorff, Brigitte Mieth, Katarina Buhl and Martin Linnemann, "Spatio-temporal gait patterns during over ground locomotion in major depression compared with healthy controls", *Journal of Psychiatric Research,* Vol. 34, No 4-5, 2000, pp. 277-283.

This is in line with the dynamic nature of the democratic constitutional state, which "evolves as a result of permanent balancing of individual, social and state interests"[756].

The 1995 Data Protection Directive constitutes the legal background of biometric technologies in Europe and establishes the legal framework against which the use of biometrics should be weighed and in which the implications of biometric technologies should be collocated. However, some critical gaps exist between the European legal framework and recent technological advances.

The current legal framework in Europe regarding the use of biometric data remains "vague", as affirmed by the Council of Europe – Committee of Legal Affairs and Human Rights Report in February this year[757], while asking member states to take further measures to improve it. If on one hand there is a tendency towards the widespread adoption of biometric technology, on the other the current legislation does not have the instruments to protect individuals against abuses and safeguard the human rights at stake. The CoE Committee Report highlighted how the rapid development of biometrics, despite the fact that they offer a solution for security concerns, "put at stake several human rights, such as the right to respect for private life, the right to a fair trial and the presumption of innocence, the freedom of movement and the prohibition of discrimination". Specific legislation is needed in this area that should: elaborate a standardised definition of "biometric data" (par. 4.1), keep the legislation under review in order to meet the challenges stemming from the further development of biometric technologies including the so called "second-generation" biometrics (par. 4.2), promote proportionality in dealing with biometric data (par. 4.3) put in place supervisory bodies (par. 4.4) and promote multi-disciplinary research on new biometric technologies. The CoE recommendations outline the main gaps between technological developments that have been described in this paper and the existing legal framework in Europe.

Second-generation biometric particularly raise the issue of the *definition of "personal data"*[758]. Several doubts have been raised on the inclusion of behavioural biometric data within this category. It is widely accepted that biometric information must be considered personal data within EU and Member States' legislation, at least if the template is associated with other personal information or if it provides a direct or indirect link to the data subject, as in concrete applications. Many behavioural and electrophysiological biometrics, however, use data which might not be classified as personal (when they are not directly linked to an identified or identifiable individual) according to Directive 95/46. Can this data, used to *target* classes of individuals (instead of to *identify* them), be classified as personal data? Which of them can be classified as sensitive – taking into account that *categorisation* of individuals may be much more sensitive than their *identification*? Some scholars have stated that that "it is also not clear whether and when profiling falls under the rights and obligations of the EC Directive 95/46"[759].

---

[756] Gurtwirth, Serge, "Biometrics between opacity and transparency", *Annali dell'Istituto superiore di sanità*, Istituto superiore di sanità, Vol.43, No. 1, 2007, pp. 61 – 65.

[757] Council of Europe, Committee on Legal Affairs and Human Rights, *The need for a global consideration of the human rights implications of biometrics*, 16 February 2011.

[758] Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2 a).

[759] De Hert, Paul, "Data Protection Implications of First and Second-generation Biometrics", in Mordini and Tzovaras, op. cit., in press.

Further concerns are raised by the shift to embedded systems and distant sensing, and the potential for *covert data capture* without the data subject knowledge or consent. The introduction of remote or covert biometrics raises particular concerns over the *individual participation principle*. According to the EU data protection directive, (art 7 par 1), no data collection can go unnoticed by the subject that is being monitored. An exception is made in par. 2, stating that par. 1 is not applied in the case of processing of data relating to offences, criminal convictions or *security measures*.

5.7 NEED FOR NEW LEGISLATION, CODES OF CONDUCT TO DEAL WITH PRIVACY IMPACTS

Since the Data Protection Directive came into force in 1995, the ways in which the personal data is accessed, collected, processed, stored and used, as well as the possibilities it is abused or misused, have seen critical changes from different points of view. These include technological issues as well as political and economic considerations. The current EU legal framework based on the 95/46/EC Directive is only partly adequate to face up these challenges to the effective protection of personal data. This is particularly in line with the challenges brought by new developments in biometrics outlined in the previous chapters.
The review of the Directive should consider the redefinition of the object of protection, possibly using a risk-based and more flexible approach[760], and reviewing the weaknesses of the current measures for the effective control of personal data flows[761]. However, considering that biometric innovation marches on rapidly, there will be some inevitable lags between technology innovation and the development of new effective regulations. In this respect, a number of other bottom up and participatory instruments are needed that can support the innovative and global governance for biometrics.

First of all, the adoption of soft law instruments that are able to support the introduction of best practices, ad hoc agreements and ethical codes of conduct, should be encouraged among those actors who are directly responsible for the information management and the processing of personal data. Bottom-up participatory instruments are particularly relevant for biometrics and privacy impact assessment tools[762], codes of conduct[763] and self-regulatory bodies[764] have been introduced in biometric systems.

---

[760] It is often said that most of the definitions clearly expressed in the Directive are technologically out of date. This concerns very critical definitions, such as "Personal Data" (in many cases it is the combination of data which renders them relatable to an "identifiable person") or "Informed Consent" (ambient intelligence and seamless communication make very difficult to apply standard procedures),

[761] The Data Protection Directive, focusing on principles and also procedures, used a typically European approach to the protection of personal data and a strict approach towards the international transfer of such data. This has also been pointed out as a paternalistic approach towards the implementation of the data protection principles, which doesn't recognize that countries would have their own legislative approaches to data protection. The current system for assessing 3rd countries is too cumbersome and lengthy, and international transfer rules are unrealistic against the globalised data flows and the needs of developing economies.

[762] See US Department of Homeland Security, "Privacy Impact Assessment for the Biometric Storage system", March 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_bss.pdf and "Privacy Impact Assessment for the US Costal Guard - Biometrics at sea", 14 Mar 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_biometrics.pdf

Secondly, in order to build up a sustainable and trustworthy ICT environment, the development of privacy enhancing technologies should also be supported. With reference to biometrics technological alternatives, technical solutions mainly include the development of privacy aware (biometric encryption, privacy by design) and privacy enhancing technologies (based on enhancing privacy sympathetic qualities of biometrics). These technical solutions are, however, relatively new to biometrics in general and even more immature for second-generation biometrics. Indeed, the existing techniques for traditional biometrics mainly exploit the relatively static nature of the raw data. If it is true that template protection has become a compulsory aspect of consideration for any biometric modality of first-generation, templates for second-generation biometrics could be more complex, depending on the number of aspects of relevance that are recorded. Initial attempts to overcome this problem have been published only recently[765].

Finally, particular attention should be given to the initiatives aiming at raising public awareness and stimulating global and multidisciplinary debate on the social, economic and technical implications related to the EU privacy and data protection legal framework applying to biometrics of first and second-generation[766].

5.8 CONCLUSIONS

Biometrics are evolving fast and have made impressive progress during the last years. The need for a reliable and convenient way of identifying individuals makes the further development of this technology inevitable. The contemporary era of biometrics is bringing about significant changes, while in many cases a lack of clarity regarding the fundamental motivations to adopt such technologies remain.

Biometrics can be used for many purposes, but many think that today's interest in the next generation of behavioural and soft biometrics is clearly augmented by society's increased surveillance needs. Because they carry the potential to free individuals from the "tyranny" of nation states in the field of personal recognition, biometrics have also been described as a "liberating" technology[767]. However, security does not seem to be the only reason for deploying these technologies, as they also seem to be increasingly adaptable to more pervasive and ambient-related uses. As the number of electronic appliances will increase in homes and of-

---

[763] See International Biometric Industry Association, "IBIA Statement of Principles and Code of Conduct". http://www.biteproject.org/documents/ibia_code_ethics.pdf

[764] An example is the Data Security Council of India (www.dsci.in), a Self Regulatory Organization created by Nasscom, the premier trade body and chamber of commerce of the IT-BPO (Business Process Outsourcing) industries in India. DSCI main mission is to facilitate the culture of security and privacy in the Indian IT industry and promote the message that India is a secure destination for outsourcing: DSCI is the only organization of its kind in the IT-BPO Industry globally. It is guided by and independent Steering Committee with balanced representation from industry and experts from the various domain of security (academia, government, law enforcement bodies and IT/ITES orgs). DSCI is partner of the RISE project on ethics of biometrics and security technologies.

[765] Argyropoulos, Savvas, Dimitrios Tzovaras, Dimosthenis Ioannis, Yannis Damousis, Michael Strinzis, Martin Braun and Serge Boverie, "Biometric template protection in multimodal authentication systems based on error correcting codes", *Journal of Computer Security*, Vol. 18, No. 1, 2010, pp. 161-185.

[766] See the EU funded initiatives HIDE (Homeland Security, Identification Technologies and Personal Detection Ethics, http://www.hideproject.org), RISE (Rising pan-European and International Awareness on Biometrics and Security Ethics, www.riseproject.eu), DETECTER (Detection technologies, counter terrorism and human rights, http://www.detecter.bham.ac.uk) projects.

[767] Mordini, Emilio, "Ethics and Policy of Biometrics", in Tistarelli, et al., op. cit., 2009.

fices, in the real as well as virtual world, so does the potential for the deployment of such technologies.

Through the analysis of continuous body dynamics, biometric data in next-generation systems can be captured in real time and at a distance, and do not necessarily require the cooperation of the individual being enrolled. While most behavioural biometrics are not unique enough to provide reliable human identification, they have been shown to provide sufficiently high accuracy for identity verification or automated classification. In general, biometric recognition of this type, based on soft or behavioural traits, requires more modalities to be consulted in order to augment the accuracy of the system, but also require more (and more sensitive) information to be collected and shared.

Technologies evolve rapidly and legal instruments can only try to stay at pace. As the deployment of next-generation behavioural, soft biometrics increases, there is an urgent need to address their potential to raise critical ethical and legal issues. These include complex questions such as:

- What are the needs met by second-generation biometrics?
- How are second-generation biometrics impacting the relationship between the state and citizens?
- How are second-generation biometrics impacting the private sphere of the individual?
- Which values and fundamental rights at are stake? Which of them are non-negotiable?
- What are the ethical implications of the possibility that in the future any human behaviour will be used as the basis for intent recognition?
- What will happen if such information is leaked outside the established context?
- How can we mitigate the risks of profiling, social sorting and discrimination?
- How can more vulnerable groups of people be protected?

5.9 REFERENCES

Abate, Andrea, Michele Nappi, Daniel Riccio and Gabriele Sabatino, "2D and 3D face recognition: a survey", *Pattern recognition letters*, Vol. 28, No. 14, 2007, pp. 1885-1906.

Al-Zubi Stephan, Arslan Brömme and Klaus D. Tönnies. "Using an Active Shape Structural Model for Biometric Sketch Recognition", *Proceedings of DAGM-Symposium,* 2003, pp.187-195.

Apap, Frank, Andrew Honig, Shlomo Hershkop, Eleazar Eskin and Sal. Stolfo, *Detecting malicious software by monitoring anomalous windows registry access*, Columbia University CS Technical Report, 2001.

Argyropoulos, Savvas, Dimitrios Tzovaras, Dimosthenis Ioannis, Yannis Damousis, Michael Strinzis, Martin Braun and Serge Boverie, "Biometric template protection in multimodal authentication systems based on error correcting codes", *Journal of Computer Security*, Vol. 18, No. 1, 2010, pp. 161-185.

Article 29 Data Protection Working Party, *Working document on biometrics*, 2003, 12168/02/EN

Biometric Technology Today*, "*Iris at a distance not yet mature enough, says UAE", Vol. 17, No. 2, Feb. 2009.

Bowyer Kevin, Karen Hollingsworth and Patrick J. Flynn, "Image Understanding for Iris Biometrics: a survey", *Computer vision and Image Understanding*, Vol. 110, No. 2, 2008, pp. 281-307

Buhan, Ileana and Pieter Hartel, "The state of the art in abuse of biometrics", University of Twente Internal Report, 2005. http://eprints.eemcs.utwente.nl/722/01/00000144.pdf

Commission de l'Ethique, de la Science et de la Technology in Québec, *In search of balance: an ethical look at new surveillance and monitoring technologies for security purposes*, Position Statement, 2008.

Cook, Diane, "Prediction algorithms for smart environments", in "Smart environments: technologies, protocols and applications", in Diane Cook and Sajal Das (eds.), *Series on parallel and distributed computing*, Wiley, 2004, pp. 175-192.

Council of Europe, Committee on Legal Affairs and Human Rights, *The need for a global consideration of the human rights implications of biometrics*, 16 February 2011.

De Hert, Paul, "Data Protection Implications of First and Second-generation Biometrics", in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.

De Hert, Paul, Scheurs Wim and Brouwer Eveline, "Machine readable identity documents with biometrics data in the EU – part III – Overview of the legal framework", *Keesing Journal of Documents and Identity,* Vol. 22, 23-26, 2007

De Marsico, Maria, Michele Nappi, Daniel Riccio and Harry Wechsler, "Iris segmentation using pupil location, linearization and limbus boundary reconstruction in ambient intelligent environments", *Journal of Ambient Intelligence and Human Computing*, No.2, 2011, p. 153-162.

Deravi, Farzin, Michael Fairhurst, R Guest, Nick Mavity and Anne Canuto, "Intelligent Agents for the Management of Complexity in Multimodal Biometrics", *Int. J. Universal Access in the Information Society*, Vol. 2, No. 4, 2003, pp. 239-304.

Deravi, F., "Biometrics everywhere. Towards effortless ambient recognition of identity", Emilio Mordini and Dmitrios Tzovaras (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.

ENISA Briefing, *Behavioural Biometrics*, January 2010. http://www.enisa.europa.eu/act/rm/files/deliverables/behavioural-biometrics

ENISA. Survey on *Security issue in virtual words.* http://www.enisa.europa.eu/act/it/oar/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/survey-on-security-issues-in-virtual-worlds

European Biometrics Portal - UNISYS, *Biometric in Europe: Trend Report,* June 2006. http://www.libertysecurity.org/IMG/pdf/Trend_Report_2006.pdf

European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

Faundez Zanui, Marcos and Monte Moreno, "State of the art in speaker recognition", *IEEE Aerospace and Electronic System magazine*, Vol. 20, No.5, 2005, pp. 7-12.

FIDIS deliverable D 7.12, "Behavioural Biometric Profiling and Transparency Enhancing Tools", 2009. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-biometric_profiling_and_transparency_enhancing_tools.pdf

French National Consultative Ethics Committee for Health and Life Sciences, *Biometrics, Identifying Data and Human Rights*, Opinion n°98, 20 June 2008.

Furl, Nicholas Jonhathan Phillips and Alice O 'Toole, "Face recognition algorithms and the other-race effect", *Cognitive Science,* Vol. 26, No. 6, 2002, pp. 797-815.

Gosh, Anup K., Aaron Schwartzbard and Michael Schatz, "Learning program behaviour profiles for intrusion detection", *Proceedings of the first USENIX workshop on intrusion detection and network monitoring*, Santa Clara, California, 1999.

Gupta, Gopal, "The State of the Art in On-line Handwritten Signature Verification", Faculty of Information Technology, Monash University, Clayton, Victoria, Australia, May 2006

Gurtwirth, Serge, "Biometrics between opacity and transparency", *Annali dell'Istituto superiore di sanità*, Istituto superiore di sanità, Vol.43, No. 1, 2007, pp.61 – 65.

International Civil Aviation Organisation Technical Advisory Group (ICAO TAG), *Biometrics Deployment of Machine Readable Travel Documents*, ICAO TAG MRTD/NTWG Technical Report, 2004

HIDE project, "BIRD Platform business model", HIDE project deliverable, 2011.

Homeland Security Market Research, *CCTV based remote biometric and behavioural suspect detection: technologies and global markets – 2011-2016*, Washington DC, 2011. http://www.homelandsecurityresearch.com/2011/02/cctv-based-remote-biometric-behavioral-suspect-detection-market-2011-2016

Ioannidis, Dimosthenis, Dimitrios Tzovaras, Gabriele Dalle Mura, Marcello Ferro, Gaetano Valenza, Alessandro Tognetti and Giovanni Pioggia, "Gait and Anthropometric profile biometrics: a step forward", in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.

International Biometric Industry Association, "IBIA Statement of Principles and Code of Conduct", http://www.biteproject.org/documents/ibia_code_ethics.pdf

Irish Council for Bioethics, "Biometrics: enhancing security or invading privacy? Opinion", The Irish Council for Bioethics, Dublin, 2009.

ISTAG Report, *European Challenges and Flagship 2020, and beyond*, Report of the ICT Advisory group, 2009.

Jain, Anil K., Sarat Dass and Karthik Nandakumar, "Can soft biometric traits assist user recognition?", *Proceedings of SPIE Defence and Security Symposium*, Orlando Florida, 2004.

Jain, Anil K., Ruud Bolle, Sharath Pankanti, *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publisher, Massachusetts, 1999.

Jain, Anil K., Sarat Dass and Karthik Nandakumar, "Soft biometric traits for personal recognition systems", *Proc. Of International Conference on biometrics authentication*, HK 731-738, 2004

Jain, A.K. P. Flynn and A.A. Ross, *Handbook of Biometrics*, Springer, New York, 2007.

Jain, A.K. and A. Kumar, "Biometrics of Next generation: an overview", in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.

Keller, Paul, "Overview of electronic nose algorithm", *International Joint Conference of Neural Networks,* Washington, DC, 1999.

Korotkyaya, Z., "Biometric person authentication: odor", *Advanced topics in Information Processing,* University of Technology, Finland, 2003.

Lemke, Mathias, Wendorff, Thomas, Mieth, Brigitte, Buhl Katarina and Linnemann, Martin "Spatiotemporal gait patterns during over ground locomotion in major depression compared with healthy controls", *Journal of Psychiatric Research,* Vol. 34, No. 4-5, 2000, pp. 277-283.

Matey, James, David Ackerman, James Bergen and Michael Tinker, "Iris recognition in less constrained environments", in N. K. Ratha and V. Govindaraju (eds.), *Advances in Biometric Sensors, Algorithms and Systems*, 2008, pp. 107-131.

Mc Carthy, Paul, "Biometric Technologies, Ethical Implications", in *Encyclopedia of Applied Ethics*, Dan Callaghan Peter Singer, Ruth Chadwick (editors in chief), 2nd Edition, Academic Press, London, 2011

Médioni, Gérard, Jongmoo Choi, Chang Hao Kuo and Douglas Fidaleo, "Identifying noncooperative subjects at a distance using face images and infrared three dimensional face models", *IEEE Trans Systems Man, Cybernetics – Part A: Systems and Humans*, Vol. 39, No. 1, 2009, pp. 12-24.

Mordini, Emilio, "Ethics and Policy of biometrics", in Massimo Tistarelli, Stan Z. Li and Rama Chellappa (eds.), *Handbook of Remote Biometrics: For surveillance and Security*, Springer, Dordrecht, 2009.

Mordini. Emilio, "Biometrics, Human Body and Medicine: A Controversial History", in P. Duquenoy, C. George and K. Kimppa (eds.), *Ethical, Legal and Social Issues in Medical Informatics*, Hershey, 2008.

Mordini, Emilio and Holly Ashton, "The Potential for Disclosure of Personal Medical Information", to appear in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.

Mordini, Emilio and Sonia Massari, "Body, Biometrics and Identity", *Bioethics*, Vol. 22, No. 9, 2008, pp. 488–498. http://www.hideproject.org/downloads/Mordini_Massari-Body_Biometrics_Identity.pdf

Mordini, E. and C. Petrini (eds.), "Ethical and Social Implications of Biometric Identification Technology", *Annali dell'ISS*, Vol. 43, No. 1, 2007.

Mordini, Emilio, *Whole Body Imaging at airport checkpoints: the ethical and political context*, HIDE&RISE policy report, February 2010 (updated March 2011). www.riseproject.eu

Most, Maxine, *The future of biometrics: Market Analysis, Segmentation and Forecast*, ACUITY Market Intelligence Report, 2009. http://www.acuity-mi.com/FOB_Report.php

Nanavati, Samir, M. Thieme, R. Nanavati, *Biometrics: identity verification in a networked world*, Wiley Ltd, 2002.

Naselaris, Thomas Ryan, J. Prenger, Kendrick, N. Kay, Michael Oliver and Jack L. Gallan, "Bayesian Reconstruction of Natural Images from Human Brain Activity", *Neuron*, Vol. 63, No. 6, 2009. http://www.cell.com/neuron/abstract/S0896-6273(09)00685-0

National Consultative Ethics Committee for Health and Life Sciences, *Biometrics, Identifying Data and Human Rights*, Opinion No. 98, 20 June 2008

National Science & Technology Council, Subcommittee in Biometrics, *The National Biometrics Challenge*, 2006

Nixon Mark, Tienu Tan and Rama Chellappa, *Human Identification based on gait*, Springer Science + Business Media, New York, 2006

O 'Toole, A.J., P.J. Phillips, A. Narvekar, F. Jiang and J. Ayyad, "Face recognition algorithms and the other-race effect", *Journal of Vision*, Vol. 8, No. 6, 2008.

Pamudurthy S., et al, "Dynamic approach for face recognition using digital image skin correlation", *Audio and video based biometric person authentication*, New York, 2005.

Pennington, Adam, John Strunk, John Linwood Griffin, Craig Soules, Garth Goodson and Gregory Ganger, *Storage-based intrusion detection: watching storage activity for suspicious behaviour*, Technical Report CMU-CS-02-179, Carnegie Mellon University, 2002.

Revett, Kenneth, *Behavioural Biometrics. A remote access approach*, Wiley Ltd, United Kingdom, 2008.

Sakar S., P. J. Phillips, Z. Liu, I. R. Vega, P. Groter and K. W. Bower, "The Human ID Gait challenge problem: data sets, performance, and analysis", *IEEE transactions on pattern analysis and machine intelligence*, Vol. 27, No. 2, pp. 162 – 177.

Schumacher, Gunther, "Behavioural biometrics: emerging trends and ethical risks", in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.

Shaun Waterman, UPI special report, "DHS wants to use human body odour as biometric identifier, clue to deception", March 2009.

http://www.upi.com/Top_News/Special/2009/03/09/DHS-wants-to-use-human-body-odor-as-biometric-identifier-clue-to-deception/UPI-20121236627329
Shipilova, Olga, *Persons recognition based on lip movements*, 2004. http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Shipilova.pdf
Spafford, Eugene H., and Stephen A. Weeber, "Software forensics: can we track code to its authors?", Purdue University Technical Report, 1992.
Stolfo, Salvatore, Chia Wei Hu, Wei-Jen Li, Shlomo Hershkop, Ke Wang, Olivier Nimesken, *Combining behavioural models to secure email systems*, Columbia University Technical report, 2003.
Tistarelli, Massimo, Susan E. Barret and Alice O'Toole, "Face Recognition, Emotion and Intention Detection: The Big Brother in the Airport?", in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.
Tistarelli, M., and B. Shouten, "Biometrics in Ambient Intelligence", *Journal of Ambient Intelligence and Human Computing*, Vol. 2, 2011, pp. 113-126.
Tistarelli, Massimo, Stan Z. Li, Rama Chellappa, *Handbook of remote biometrics for surveillance and security,* Advances in Pattern Recognition Series, Springer-Verlag, London, 2009.
Tistarelli, M., and B. Shouten, "Biometrics in Ambient Intelligence", *Journal of Ambient Intelligence and Human Computing*, Vol. 2, pp. 113-126, 2011.
van der Ploeg, Irma, "Security in the danger zone: normative issues of next generation biometrics", in Mordini E, Tzovaras D (eds.), *Second-generation Biometrics: the Ethical and Social Context*, Springer, in press.
van der Ploeg, Irma, *The Machine Readable Body. Essays on biometrics and the Informatization of the body*, Shaker, Germany, 2005
Velastin, S. A., L. Khoudour, B. P. L. Lo, J. Sun and M. A. Vicencio-Silva, *Prismatica: a multi-sensor surveillance system for public transport networks,* 2004. http://eprints.ucl.ac.uk/1355/1/2004_48.pdf
US Department of Homeland Security, "Privacy Impact Assessment for the Biometric Storage system", March 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_bss.pdf
US Department of Homeland Security, "Privacy Impact Assessment for the US Costal Guard - Biometrics at sea, 14 March 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_biometrics.pdf
US National Science and Technology Council, SubCommittee on Biometrics, *The National Biometric Challenge*, August 2006.
Yampolskiy, Roman and Venu Govindaraju, "Behavioural biometrics: a survey and classification", *International Journal of Biometrics* (IJBM), Vol. 1, No. 1, 2008, pp. 81 – 113.
Yanushkevich, Svetlana, Adrian Stoica, Vlad Shmerko and Denis Popel, *Biometric Inverse Problems*, CSC Press Taylor & Francis Group, Boca Raton FL, 2005.
Westein et al., "Biometric identification using song-based eye blink patterns", *Human Computer Interaction International*, Las Vegas, 2005.
Westeyn, Tracy, Peter Pesti, Kwang-Hyun Park and Thad Starner, "Biometric identification using song-based eye blink patterns", *Human Computer Interaction International*, HCCI, Las Vegas NV, 2005. http://www.cc.gatech.edu/~thad/p/031_30_Gesture/biometric_ID_HCII05.pdf
Wang Lai-Xi and X. Geng, "Behavioural biometrics for human identification: intelligent applications", *Medical Information Science Reference*, IG Global, 2009

Wickins, Jeremy “The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification”, *Science and Engineering Ethics*, Vol. 13, 2004, pp. 45-54.

Zhao, W., R. Chellappa, P. J. Phillips and A. Rosenfeld, “Face recognition: a literature survey”, *ACM Computing Surveys*, Vol. 35, No. 4, December 2003, pp. 399–458.

Chapter 6, Privacy, data protection and policy issues in next generation DNA sequencing technologies

Piret Kukk, Bärbel Hüsing and Michael Friedewald
Fraunhofer ISI

6.1 INTRODUCTION TO THE FIELD

The blueprint of how a living organism is built and how it functions is laid down in the genetic material that is contained in every cell of an organism. For decades, it has been a goal in biological research to crack the genetic code and decipher the genetic information of living organisms. The findings that genetic material is made up of a linear, double-helix-shaped macromolecule, desoxyribonucleic acid (DNA) which consists of four different monomeric building blocks, the nucleotides, and that genetic information is coded in the exact sequence of these four nucleotides in the macromolecule were awarded the Nobel prizes for Medicine in 1962 and 1968, respectively.

Since the 1970s, wet chemical methods have been developed and applied in order to determine the sequence of genes and full genomes of various species. The largest of these endeavours was the sequencing of the three billion nucleotides of a human genome. The first draft of the sequence of a human genome was published in 2001[768], the final sequence in 2004[769]. A prerequisite for the successful completion of the first human genome sequence was the significant improvement, automatisation and miniaturisation of the DNA sequencing method. In the last decade, DNA sequencing technologies have been further improved considerably, raising speed and throughput by several orders of magnitude and decreasing costs significantly: While it took 14 years, international cooperation and $3 billion USD to completely sequence a human genome for the first time, with improved technologies this can now be accomplished in a matter of weeks at costs of a few thousand USD. Experts are of opinion that by 2015 it will become possible to sequence the genome of an individual human at costs of approximately $1,000 USD in a few hours to days.

Improvements in sequencing technology have positioned DNA sequencing at the forefront of biological experimentation and have changed research approaches. Today, as whole genome sequencing is becoming more affordable, the promise of large-scale human genomic research studies involving thousands and even tens of thousands of patients is becoming a reality.[770] Research projects all over the world are generating genomic data by genotyping or sequencing the genomes of their participants. This is happening in the research community and in the private sector; sequence data are now being generated by a number of private companies which offer direct to consumer genetic testing and, in some cases, feedback raw sequence data as well as their interpretation of it.[771] Although the ability to share and access genomic data is vital to the progress of scientific research, the implications that a lack of protection of privacy could have for the lives of individuals and the whole society should not be forgotten.[772]

Genetic information is sensitive personal information. It does not only give information about the person from whom the DNA was taken, but also about the person's relatives. Today, DNA sequencing is mainly applied in biomedical and biological research and in diagnosis in human

[768] Venter, J. Craig, Mark D. Adams, Eugene W. Myers, et al., "The sequence of the human genome", *Science*, Vol. 291, No. 5507, 2001, pp. 1304-1351. The International Human Genome Sequencing Consortium, "Finishing the euchromatic sequence of the human genome", *Nature*, Vol. 431, No. 7011, 2004, pp. 931-945.
[769] The International Human Genome Sequencing Consortium, op. cit., 2004.
[770] Lunshof, Jeantine E., Jason Bobe, John Aach, et al., "Personal genomes in progress: from the human genome project to the personal genome project", *Dialogues in Clinical Neuroscience*, Vol. 12, No. 1, 2010, pp. 47-60.
[771] Kaye, J., "The regulation of direct-to-consumer genetic tests", *Human Molecular Genetics*, Vol. 17, No. 2008, pp. R180-R183.
[772] Heeney, Catherine, N. Hawkins, J. de Vries, et al., "Assessing the Privacy Risks of Data Sharing in Genomics", *Public Health Genomics*, Vol. 14, No. 1, 2011, pp. 17-25.

genetic medicine. DNA profiling, a method to analyse genomic DNA which differs from DNA sequencing, is widely used. In order to establish paternity and other family relationships and in criminal investigations for forensic purposes, genomic DNA is also analysed. Here, the method of choice is DNA profiling, yielding less information than DNA sequencing, but could be complemented in the future by DNA sequencing as well.

DNA sequencing and DNA analysis are presently governed by regulations which are based on the assumption that these are mainly confined to research and human genetics in health care. The regulations aim at safeguarding data protection and privacy, especially autonomy and the right not to know in the context of genetic testing for diagnostic medical purposes. However, due the dynamic development of DNA sequencing technologies, the following quantitative and qualitative changes in genome analysis can be expected in the coming decade:

- Higher frequency of DNA sequencing than today and on a routine basis
- Revelation of much more information than before, because no longer only selected genes, but whole individual genomes will be sequenced
- New applications in basic and biomedical research
- Establishment as a routine diagnostic method in health care
- Applications outside basic research and biomedical research, use by different players and for different purposes, compared to today

This will challenge both understandings of genetic privacy as well as existing regulations and ethical principles regarding data protection and handling of genetic information.

This paper will discuss and analyse the following issues:

- Description of the DNA sequencing technology;
- State-of-the-art analysis of second-generation DNA sequencing technologies;
- Examinations of actors involved in the development of the DNA sequencing technologies;
- Possible privacy infringements arising from next-generation DNA sequencing technologies;
- Extent to which existing rules and processes can be applied;
- Conclusions.

6.2 CURRENT STATUS OF THE DNA SEQUENCING TECHNOLOGY AND EXPECTED PROGRESS

6.2.1 Introduction into DNA sequencing and sequence analysis

Genetic information is laid down in the exact sequence of the four building blocks (nucleotides) in the DNA macromolecule. Several wet chemistry methods have been developed to determine the sequence of the four building blocks along the DNA strand; these are DNA sequencing methods. Such a sequencing exercise results in a series of nucleotide names (e.g. AATTCGATGGGA...) which can be stored in digital form and be analysed further in silico.

A DNA sequence as such is of little value unless the “meaning” or function that is encoded in this DNA sequence is known. Therefore, a major challenge in molecular genetics is the elucidation of the functions which are being coded by the respective DNA sequences (functional genomics). For any applications of whole genome sequencing, the sequencing exercise must be followed by an analysis of these raw data. This is done by applying software which inte-

grates the latest scientific knowledge of the relationship between DNA sequence and biological function (e.g. health, disease and non-medical traits).[773]

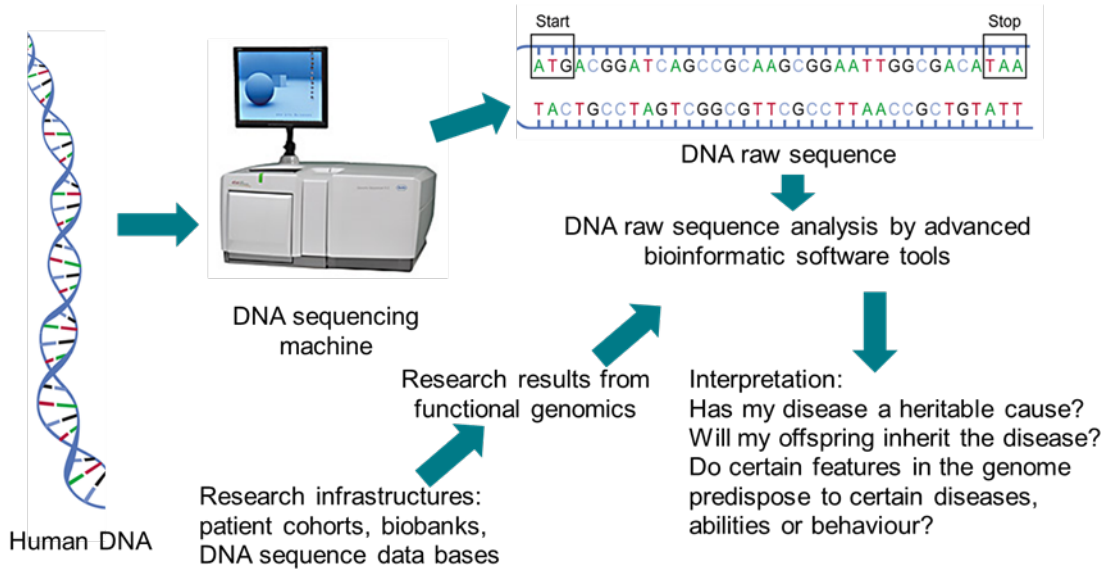


Figure 6.1: Principle of DNA sequencing and DNA sequence analysis

6.2.2 *The first wave of DNA sequencing – Sanger technique*

The method of choice for DNA sequencing is the so called Sanger technique, named after its inventor, Frederick Sanger. It was developed in the late 1970s[774] and has become and remained the gold standard against which new technologies are being compared. The technology that was applied around 2000 to sequence the first human genome was also based on Sanger methodology. Because of the increased scale required especially for the Human Genome Project, genome centres at the time had developed a robust, highly automated and inexpensive preparatory process to feed their capillary sequencers. During that period, sequence production, not sequence analysis, was the rate limiting factor.[775] The Sanger technique/chemistry is rapid, robust, has >99.9% raw base accuracy (the frequency in which the instrument correctly identifies a nucleotide from a known template sequence), and can typically achieve read lengths of up to 1-1.2 kb, however, it still cannot read 2 kilo base pair beyond the sequencing primer.[776], Therefore, it is adequate for the majority of clinical applications involving the analysis of single genes with limited polymorphism. However, for many clinical applications such as the detection of somatic gene mutations in solid tumours or acute leukaemia, the level of sensitivity afforded by the Sanger technique (generally estimated at 10-20%) may be insufficient for detection of clinically relevant low-level mutant alleles or organisms. Also, the experience of sequencing the human genome had demonstrated that the Sanger technique was not readily scalable to achieve a throughput capable of efficiently ana-

[773]Health Council of the Netherlands, Wybo J. Dondorp, and Guido M.W.R. de Wert, "The 'thousand-dollar genome': an ethical exploration", Monitoring Report Ethics and Health 2010/2, Centre for Ethics and Health, The Hague, 2010. http://www.gezondheidsraad.nl/en/publications/thousand-dollar-genome-ethical-exploration.
[774] Sanger, F., S. Nicklen and A.R. Coulson, "DNA sequencing with chain-terminating inhibitors", *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 74, No. 12, 1977, pp. 5463-5467.
[775] Mardis, E. R., "The impact of next-generation sequencing technology on genetics", *Trends in Genetics*, Vol. 24, No. 3, 2008, pp. 133-141. Zhang, J., R. Chiodini, A. Badr, and G. Zhang, "The impact of next-generation sequencing on genomics", *Journal of Genetics and Genomics*, Vol. 38, No. 3, 2011, pp. 95-109.
[776] Anderson, Matthew W., and Iris Schrijver, "Next Generation DNA Sequencing and the Future of Genomic Medicine", *Genes*, Vol. 1, No. 1, 2010, pp. 38-69. Zhang, et al. ,op. cit., 2011.

lysing complex diploid genomes at low cost, as sequencing the first genomes with this method cost several billion US dollars, mobilised hundreds of scientists all over the world and was extremely labour intensive.[777]

6.2.3 State of the art of DNA high throughput sequencing technology

An ideal DNA sequencing platform would allow to sequence long stretches of DNA in a high-throughput, rapid manner and with high accuracy. Long-read lengths are favourable since they would significantly decrease the computational power required to perform genome assembly. There are several technologies available for new generation high-throughput DNA sequencing that outperform the older Sanger-sequencing technologies by a factor of 100-1000 in daily throughput (see Figure 1), making it possible to sequence entire human genomes in a matter of weeks and at the same time reduce the cost of sequencing one million nucleotides to 4-0.1% of that associated with Sanger sequencing.[778] The examples of high throughput sequencing instruments commercially available include new instruments from Roche (454), Illumina (Genome Analyzer IIx), Life Technologies (SOLiD), Helicos Biosciences (Heliscope) and Complete Genomics Platform.[779] The availability of several commercially available instruments alone represents a paradigm shift from the previous decade, where a single capillary instrument produced by Applied Biosystems dominated the market.

These commercially available next generation sequencing platforms differ from traditional Sanger sequencing technology in a number of technological ways.[780] First, the DNA sequencing libraries are clonally amplified *in vitro*, obviating the need for time consuming and laborious cloning of the DNA library into bacteria. Second, the DNA is sequenced by synthesis, such that the DNA sequence is determined by the addition of nucleotides to the complementary strand rather than through chain termination chemistry (as in the Sanger method). Finally, the spatially segregated, amplified DNA templates are sequenced simultaneously in a parallel fashion without the requirement for a physical separation step.[781] While these above described advances are shared across all commercially available high-throughput sequencing platforms, each of them utilises a slightly different strategy as explained in Table 1.

With these next-generation sequencing platforms, a human genome in the resolution of 100 GB can currently be sequenced for $45,000 USD (including reagent, equipment and labour), with the potential to drive costs further down to $1,000 to 5,000 USD[782]. In addition, the next-generation DNA sequencing instruments are so powerful that no longer sequence production, but sequence analysis has become the bottleneck.

[777] Venter, et al., op. cit., 2001,.
[778] Kircher, M., and J. Kelso, "High-throughput DNA sequencing - concepts and limitations", *Bioessays*, Vol. 32, No. 6, 2010, pp. 524-536.
[779] Koboldt, D. C., L. Ding, E. R. Mardis and R. K. Wilson, "Challenges of sequencing human genomes", *Briefings in Bioinformatics*, Vol. 11, No. 5, 2010, pp. 484-498.
[780] Zhang, et al., op. cit., 2011.
[781] Anderson and Schrijver, op. cit., 2010.
[782] Babiel, Rainer, "Personal communication during the workshop 'Privacy issues arising from next generation whole genome sequencing'", Brussels, 1 June 2011.

	Roche/454 Life Sciences	Applied Biosystems/ SOLiD	Illumina	Pacific Biosciences
Amplification method	Emulsion PCR	Emulsion PCR	Ensymatic bridge amplification	Not applicable
Sequencing method	Polymerase mediated	Ligation based	Polymerase mediated	Polymerase mediated
Time/run	7 h	5 days	4 days	
Detection method	Light emission	Fluorescent emission	Fluorescent emission	Fluorescent emission
Error model	Insertion/ deletion errors	End of read sub-stitution errors	End of read sub-stitution errors	Insertion/ deletion errors
Read length	400 bp	75 bp	150 bp	>1000 bp
Cost per Mb	80 USD	6 USD	6 USD	
Strengths	Long read, short run time	Software open source, cheaper		
Weakness	Low throughput, highest cost per base		Low quality on longer runs	15 % error rate (single reads)

Table 6.1: Next generation sequencing platforms comparison[783]

6.2.4 "Third-generation" DNA sequencing

On the way to an ideal DNA sequencing platform, significant advances are expected from the adoption of new technologies, e.g. nanotechnologies, electron microscopy, or semiconductor technologies, leading to so called powerful "3rd generation DNA sequencing technologies". Among them are single molecule DNA sequencing technologies which bear the potential to deliver whole human genome sequencing at less than $1,000 USD per genome when becoming commercially available from 2015 onwards. The Helicos HeliScope platform is the first single molecule sequencing technology already commercially available (Table 6.1) and others are currently under development; however, little information has been made publicly available[784]. They are based on the principle that the nucleotide sequence is being read directly when driving individual DNA molecules through a nanopore electrophoretically or by monitoring an individual polymerase molecule in real time as it synthesises DNA.[785] As these real time systems are capable of delivering sequencing data from single molecules of DNA as they are being sequenced – rather than as a stepwise series of nucleotide addition steps that are analysed after the sequencing instrument has finished – the time for the sequence data generation step is shortened significantly relative to next-generation systems. One such instrument from Pacific Biosciences that is being tested in early access sites monitors each one of an array of individual polymerases while DNA synthesis is occurring, in order to obtain the single molecule sequences in a minimum of 30 minutes. Other instruments in development, including those by Oxford Nanopore or IBM/Roche, use nanopore technology to identify individual DNA nucleotides as the DNA fragment passes through the nanopore by one of several detection approaches. Although the current capacities of real-time sequencers would not permit whole human genome sequencing in a single run, the near-term application of these instru-

[783] For the latest information, see: http://knowledgebank.blueseq.com/sequencing-platforms/comparison-of-sequencing-technologies/
[784] Babiel, op. cit., 2011.
[785] Branton, D., D. W. Deamer, A. Marziali, et al., "The potential and challenges of nanopore sequencing", *Nature Biotechnology*, Vol. 26, No. 10, 2008, pp. 1146-1153.

ments could be on focused evaluation of specific human genes or on the genomes of pathogens for diagnosis, prognosis or therapeutic prescription.[786].

Table 6.2 summarises the progress in DNA sequencing that has been achieved in the past 30 years and how it is expected to continue. If one compares this development in sequencing technology with computer hardware development, in the last years DNA sequencing has developed faster than Moore's Law, which describes the performance improvement in computer hardware.

	Classical	**Human Genome Project**	**Next-generation sequencing**	**Third-generation sequencing**
Period	Before 1990	1990 - 2004	2005 - 2011	2015 +
Technology	Sanger	Sanger, automated, improved		Single molecule sequencing
DNA sequenced	1 gene	1 reference genome	1 individual genome	1 individual genome
Time	3 years	10 (14) years	weeks	week
Costs		$3 billion USD	$45,000 – 50,000 USD	$1,000 USD

Table 6.2: Overview of progress in DNA sequencing technologies in three decades

[786] Mardis, E. R., "A decade's perspective on DNA sequencing technology", *Nature*, Vol. 470, No. 7333, 2011, pp. 198-203.

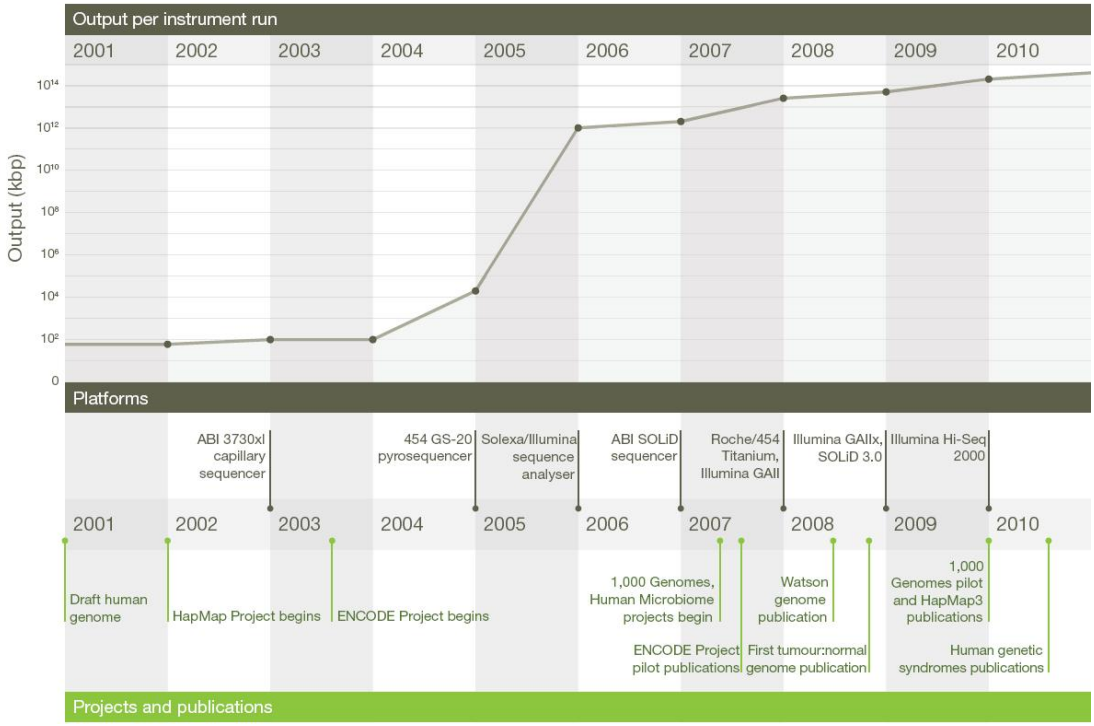


Figure 6.2: Changes in instrument capacity over the past decade and timing of the major sequencing projects[787]

6.3 NEXT AND THIRD-GENERATION DNA SEQUENCING APPLICATIONS

6.3.1 High throughput sequencing uses in research

Presently, the most important and diverse applications of genome sequencing and next-generation sequencing technologies have been in research. The rise of new-generation sequencing technologies has changed the practice of biology in fundamental ways (e.g. the ability to investigate biological phenomena in a comprehensive, unbiased, hypothesis-free manner, e.g. due to genome-wide approaches) and rapidly accelerated biomedical research.[788] A large body of research aims at elucidating the complex relationship between genetic variation, environmental factors and health. The ability to cheaply and quickly sequence complete genomes for individuals is an important tool in this endeavour.

In the following paragraphs, we outline the research agendas for the coming decade in which next and third-generation sequencing will play a crucial role:[789]

- Understanding of all functional elements encoded in the human genome. The goal is to characterise complete genomes, transcriptomes[790] and epigenomes[791] for research purposes. This

[787] Ibid.

[788] Zhang, et al., op. cit., 2011.

[789] Kukk, Piret, and Bärbel Hüsing, "Privacy, data protection and policy implications in whole genome sequencing", in van Est, Rinie, and Dirk Stemerding (eds.), *Making Perfect Life. Bio-engineering (in) the 21st Century. Deliverable No. 5 of the STOA Project "Making Perfect Life"*, Rathenau Institute, The Hague, 2011, pp. 37-70. Lander, E. S., "Initial impact of the sequencing of the human genome", *Nature*, Vol. 470, No. 7333, 2011, pp. 187-197.

[790] The transcriptome is the set of all RNA molecules in a given organism or cell type. It reflects the set of genes that are being actively expressed. Unlike the genome, which is stable over time, the transcriptome may change considerably with physiological state, environment, age and cell type.

can only be done by parallel, low-cost DNA sequencing of all protein-coding and non-protein coding genes and transcripts and all epigenomic modifications and by assay miniaturisation for molecular interactions.

- Creation of a catalogue of all genetic variants in the genomes of humans. While the vast majority of variants with frequencies > 5 per cent in human genomes have been discovered, and 95 per cent of heterozygous SNPs in an individual are represented in current databases, less frequent variants have so far escaped detection with conventional approaches and technologies. Therefore, next- and third-generation re-sequencing of human genomes from different ethnicities will be key to setting up a catalogue of genetic variants with a frequency of > 1 per cent across the genome and > 0.1 per cent in protein-coding regions. Projects such as the 1000 Genomes Project (www.1000genomes.org) contribute to this goal.
- Identification of disease genes for (rare) Mendelian diseases. There are approximately 3,000 inherited disorders caused by defects in single – yet still unknown – genes. In addition to the analysis of families in which the respective diseases are prevalent, systematic next-generation genome (exome) sequencing of parents and offspring offers an additional approach for identifying these genes. Moreover, it is expected that multifactorial common diseases can also be addressed by this strategy. On the one hand, many rare Mendelian diseases hide among complex diseases due to similar symptoms; on the other hand, causative or mechanistic insight gained from rare diseases may also guide future research into multifactorial diseases.[792]
- Identification of disease genes and pathways of common, multifactorial diseases. One strategy is to combine large genome-wide association studies with whole genome sequencing, which will also be informed by results from studying rare inherited disorders.
- Identification of all genes that are significant targets of somatic alterations in all human cancer types. Large-scale international projects (e.g. Cancer Atlas and the International Cancer Genome Project) have been set up to detect somatic mutations in cancers by sequencing the entire tumour DNA. This information is expected to lead to new and additional diagnostic methods and to inspire the development of new small molecule cancer drugs specifically targeting the mutated cancer cell functions. It will hopefully lead to improved cancer therapies. In the medium to long term, genomic variants of tumour DNA as well as variants in the patient's (host's) genome will need to be studied in order to achieve personalised cancer therapies.

All over the world, many projects – often the cooperation between large international consortia – have been set up, which aim at collecting the relevant biological samples and health information, gather the relevant data and analyse them according to the research priorities listed above. The promise of large-scale human genomic research studies involving thousands participants is slowly becoming a reality[793]. However the acceleration of whole-genome sequencing in the research context demands new perspectives and governance models, if increasing datasets are to explored for research without compromising the established ethical, legal and social norms.[794] Among those numerous projects are two projects which will explicitly perform whole genome sequencing of individuals: The "1000 Genomes Project" and the "Personal Genome Project".

---

[791] The epigenome is the set of heritable changes in gene expression caused by mechanisms other than changes in the DNA sequence, e.g. by DNA methylation or histone deacetylation.

[792] Check Hayden, Erika, "Genomics shifts focus to rare diseases", *Nature*, Vol. 461, No. 7263, 2009, pp. 458-459.

[793] Zhang, et al., op. cit., 2011.

[794] Lunshof, et al., op. cit., 2010.

The 1000 Genomes Project is the first project to sequence the genomes of a large number of people in order to provide a comprehensive resource of genetic variations in humans. The project is designed to enable the discovery of most genetic variants that have frequencies of at least 1 per cent in the populations studied.

The Personal Genome Project[795], announced in 2006, goes beyond the 1000 genomes project, as it links genomic with phenotypic data. It is a research study that aims to develop a database of 100,000 entries, as an open genomic resource, that would be publicly accessible for both researchers and participants. The project will publish the genotype of the volunteers, along with extensive information about their phenotype: medical records, various measurements, MRI images, etc. Such integrated data collections are important drivers of progress in functional genomics and enable systems biology based insights into the mechanisms of human health and disease.[796] All this data will be freely available over the Internet, so that researchers can test various hypotheses about the relationships among genotype, environment and phenotype. In October 2008, the first set of DNA sequences was published of ten participants, and by February 2010, more than 12,000 individuals willing to participate in this study had registered.

An important part of the project is the analysis of ethical, legal and social issues and challenges, associated with large-scale whole genome sequencing, especially in the areas of privacy, informed consent and data accessibility.[797] The Personal Genome Project (PGP) is characterised by some specific attributes when exploring the legal and social issues around it, such as integrated data, which means that the various types of genomic and phenotypic data about any project participant are accessible in a linked format. Promises of perfect privacy, anonymity or confidentiality are not realistic within this kind of research model; therefore participants are made aware of the possibility that they could be identified with their publicly available data.[798] Another characteristic is open access, as data sets and tissues are made publicly available with minimal or no access restrictions, and are, in principle, transferable outside the original research study or individual.[799] These two issues require that a premium has to be placed on receiving truly voluntary and informed consent from participants in public genomics research projects. In order to pursue this kind of innovative research in a responsible manner, the PGP has developed a number of project specific tools and resources, as the practice of public genomics is forcing the research community and policy-makers to critically reassess current organisation and governance frameworks and practices.[800] As an example, the open-consent model has been developed for the PGP. It opts for openness in its scientific design and for veracity as the leading principle in obtaining participant consent.[801]

6.3.2 Next generation sequencing applications in health care

Presently, DNA sequencing is only performed in health care if a Mendelian genetic disease is suspected based on family medical history or clinical symptoms. Guidance, ethical and regulatory frameworks governing genetic counselling and quality assurance for this type of ge-

[795] http://www.personalgenomes.org
[796] Drmanac, R., A. B. Sparks, M. J. Callow, et al., "Human Genome Sequencing Using Unchained Base Reads on Self-Assembling DNA Nanoarrays", *Science*, Vol. 327, No. 5961, 2010, pp. 78-81.
[797] Lunshof, et al., op. cit., 2010.
[798] Ibid.
[799] Ibid.
[800] Ibid.
[801] Lunshof, Jeantine E., Ruth Chadwick, Daniel B. Vorhaus, and George M. Church, "From genetic privacy to open consent", *Nature Reviews Genetics*, Vol. 9, No. 2008, pp. 406-411.

netic analysis have been established in recent years. DNA sequencing is only performed in a targeted fashion in narrowly confined parts of the genome (e.g. single or a few genes) that are the known causes of the genetic disease to be diagnosed. Usually, the traditional Sanger sequencing technology is applied and costs are in the order of magnitude of a few thousand Euros (€). Sequencing technology providers are of the opinion that molecular testing or sequencing a limited set of genes or mutations will remain the desired diagnostic format in health care in the next 5-10 years[802].

Next-generation sequencing machines are currently being installed in hospital settings, thus establishing the technical prerequisites for whole genome sequencing in health care settings. Applications of next-generation sequencing are already performed in clinical research projects or on a case by case basis. They may soon be translated into clinical practice: among them are genome-wide sequencing of tumours to detect somatic mutations that drive the tumour growth and give clues for tumour staging, selection of the most appropriate drug therapy and prediction of disease course and outcome. Moreover, genome-wide diagnostic testing is performed in cases where diseases have an unexplained cause, e.g. mental retardation in children[803]. According to experts from science and technology, DNA microarrays that are currently being applied for diagnosing chromosomal imbalances in diagnosing developmental delay, intellectual disability, autism and birth defects[804] could soon be replaced by whole genome (exome) sequencing in the coming years.

Moreover, the science and technology community of genomics and whole genome sequencing is increasingly advocating genome-wide screening. In contrast to genome-wide diagnostic testing, genome-wide screening is performed without a concrete medical indication or purpose. In principle, genome-wide screenings could be performed on any human genomic DNA. The following cases of genome-wide screenings can be distinguished[805]:

- Adults. Genome-wide screening of adults is often advocated as a part or even a prerequisite of the vision of personalised medicine[806]. Benefits for the individual could be lifestyle advice, early detection of diseases, detection of carrier status, and input into reproductive decisions. Genome-wide screenings are already offered by more than 30 private companies worldwide for several thousand Euros. Many of these companies operate on a direct-to-consumer (DTC) basis, i.e. without the involvement of a health care provider[807], outside the classical doctor-patient relationship, on a private contractual, commercial basis. However, it is not known how many people are using genetic profiling services and whether this is lead-

[802] Babiel, op. cit., 2011.
[803] Ropers, Hans Hilger, "Genetics of Early Onset Cognitive Impairment", *Annual Review of Genomics and Human Genetics*, Vol. 11, No. 2010, pp. 161-187. Najmabadi, H., H Hu, M. Garshasbi, et al., "Deep sequencing reveals 50 novel genes for recessive cognitive disorders", *Nature*, Vol. 478, No. 7367, 2011, pp. 57-63.
[804] Lander, op. cit., 2011.
[805] Kukk and Hüsing, op. cit., 2011.
[806] Hüsing, Bärbel, Juliane Hartig, Bernhard Bührlen, et al., "Individualisierte Medizin und Gesundheitssystem. Zukunftsreport", TAB-Arbeitsbericht 126, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Berlin, 2009.
[807] Hennen, Leonhard, Arnold Sauter and E. van den Cruyce, "Direct to consumer genetic testing", Final Report IP/A/STOA/FWC/2005-28/SC 39, European Parliament, DG Internal Policies, Policy Department A: Economic and Scientific Policy, STOA, Brussels, 2008. Javitt, G., "Which way for genetic-test regulation? Assign regulation appropriate to the level of risk", *Nature*, Vol. 466, No. 7308, 2010, pp. 817-818.

ing to any actual harm. However, there are several downsides of DTC genome-wide screening[808]:

- The test results can be unreliable and difficult to interpret.
- "Good" results may lead to complacency in lifestyle.
- Learning about risk of disease could be upsetting, particularly if no treatments are available.
- People may seek unnecessary further tests or advice from their doctor.
- There is a potential for misuse of personal genetic information, because there is no overview or control over how the complete and detailed data sets are stored electronically, which presents a threat to privacy of the individuals whose data is used in DTC testing.[809] There is consensus in the scientific community that the utility of such genetic profiling services for the customer presently is very low to non-existing and "not worth the money". There is also evidence that children's DNA is already analysed in this way by various companies. This, however, does not comply with established professional standards of genetic testing in minors.[810]

• Children. Screening of new-borns or children would be motivated by the assumption that the benefits of genome-wide screenings could be harnessed best if genomic information were collected as early as possible in life, and the established neonatal heel prick screening could be used to obtain samples for whole genome sequencing of neonates. This would contradict established professional guidelines, which state that for predictive genetic testing, the availability of therapeutic or preventive measures is necessary for testing to be performed in asymptomatic minors.

• Prenatal screening. It is technically feasible to expand established invasive prenatal diagnostic genetic testing procedures for indicated conditions to whole genome/exome screening approaches. Moreover, research is well underway to extract foetal DNA from maternal blood, so that the risky, invasive procedure of aspiring foetal cells will no longer be required.[811] Thus, these two developments may act synergistically to technically lower the threshold to perform whole genome prenatal screening on a routine basis.[812]

• Pre-implantation genetic screening. Pre-implantation genetic screening (PGS) of in vitro embryos is done in order to select embryos for transfer that promise the highest probability of implanting in the uterus, thus improving the success rates for in vitro fertilisation, and to reject embryos that show developmental or genetic abnormalities[813]. The technologies presently employed in screening could be complemented or even replaced by whole ge-

[808] Weale, Albert, Hugh Perry, et al., "Medical profiling and online medicine: the ethics of 'personalised healthcare' in a consumer age", Nuffield Council on Bioethics, London, 2010.
[809] Javitt, op. cit., 2010.
[810] Howard, H.C., D. Avard and P. Borry, "Are the kids really all right? Direct-to-consumer genetic testing in children: are company policies clashing with professional norms?", *European Journal of Human Genetics*, Vol. 19, No. 11, 2011, pp. 1122-1126.
[811] Go, A. T. J. I. , J. M. G. van Vugt and C. B. M. Oudejans, "Non-invasive aneuploidy detection using free fetal DNA and RNA in maternal plasma: recent progress and future possibilities", *Human Reproduction Update*, Vol. 17, No. 3, 2011, pp. 372-382.
[812] Greely, Henry T., "Get ready for the flood of fetal gene screening", *Nature*, Vol. 469, No. 7330, 2011, pp. 289-291.
[813] Harper, J.C., E. Coonen, M. De Rycke, et al., "ESHRE PGD consortium data collection X: cycles from January to December 2007 with pregnancy follow-up to October 2008", *Human Reproduction Update*, Vol. 25, No. 11, 2010, pp. 2685-2707.

nome/exome sequencing. However, there is no evidence of a beneficial effect of PGS as currently applied on the live birth rate after IVF[814].

6.3.3 Forensics

One of the established uses of genetic material analysis is in forensics for the identification of individuals. It is mainly used for the following purposes[815]:
- to identify potential criminals whose DNA may match evidence left at crime scenes;
- to exonerate persons wrongly accused of crimes;
- to identify crime and catastrophe victims, and
- to establish paternity and other family relationships.

DNA fingerprints vs. whole DNA sequencing

The method currently employed here is forensic DNA profiling[816]. It differs significantly from whole genome sequencing with respect to the quality of information that can be gleaned from the analysis of DNA. A DNA profile is not based on the whole sequence of the DNA. Rather, it is based on the finding that human DNA contains certain regions in which repetitive stretches of short base sequences (so called short tandem repeats, STR) can be found. The number of repetitions in these regions varies from individual to individual. If the number of repetitions is determined at 8-13 loci, distributed over the entire genome, a DNA profile will result which is specific for this individual. The chance that any randomly chosen person in the population at large would have the same profile is one in one billion. If a DNA profile of unknown identity or origin is compared to other DNA profiles of known identity, with statistical support, a profile match provides strong evidence for individual identification (except for monozygotic twins), whereas a mismatch does not[817]. Because DNA is shared with relatives, a person's DNA profile can be used to identify parents or children, and even more distant relatives, with certain probabilities. DNA profiles do not allow personal characteristics of a person to be inferred, or only to a limited extent: biogeographic ancestry may be deduced because profiles are much more common in certain populations and an exception in others. When applying additional methods of forensic DNA phenotyping, information about sex and statistical interpretations about phenotypic traits may be provided.[818]

Increasing number of databases worldwide

DNA profiles are usually stored in forensic databases as a digital number code: the string of numbers is based on the number of repeats at each of the tested DNA loci. Forensic databases usually contain DNA profiles from two different sources: crime scene DNA samples and individuals' DNA samples. These national DNA databases are usually used to match crime scene samples to profiles in the database. They also allow "speculative searching", yielding

[814] Mastenbroek, S., M. Twisk, F. van der Veen and S. Repping, "Preimplantation genetic screening: A systematic review and meta-analysis of RCTs", *Human Reproduction Update*, Vol. 17, No. 4, 2011, pp. 454-466.
[815] http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml
[816] Jeffreys, A.J., V. Wilson and S.L. Thein, "Individual-specific 'fingerprints' of human DNA", *Nature*, Vol. 316, No. 6023, 1985, pp. 76-79.
[817] Jobling, M.A., and P. Gill, "Encoded evidence: DNA in forensic analysis", *Nature Reviews Genetics*, Vol. 5, No. 10, 2004, pp. 739-751. Kayser, M., and P. de Knijff, "Improving human forensics through advances in genetics, genomics and molecular biology", *Nature Reviews Genetics*, Vol. 12, No. 3, 2011, pp. 179-192.
[818] Kayser and de Knijff, op. cit., 2011.

new suspects for the crime for further criminal investigation[819]. Worldwide, at least 120 countries use DNA profiling in criminal investigations, 54 countries have established forensic national DNA databases with at least 16 million DNA profiles, additionally 26 countries plan the setting up of new DNA databases.[820] As of January 2010, the United States has the largest forensic DNA database in the world with over 7.8 million offender DNA profiles and over 300,000 forensic profiles. The second largest DNA database worldwide is in the United Kingdom, the UK Police National DNA Database, with over 5 million DNA profiles.[821] As of January 2009, DNA databases throughout Europe contained over 6.8 million offender profiles, over 750,000 crime scene profiles and database searches have yielded over 1.2 million matches (crime scene to crime scene and crime scene to suspect), but over 4 million of the offenders included are from the United Kingdom as are over 900,000 of the matches. There are plans to set up new databases or expand existing databases in many countries, e.g. by collecting DNA profiles from the entire population (e.g. Arab Emirates, Uzbekistan, Bermuda, Pakistan).

Transfer of information across international borders

Data-sharing, involving the transfer of information across international borders, is also on the increase.[822] In 2005, Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria signed the Prüm Treaty. It – among others – allows direct access by the law enforcement agencies in the participating states to the forensic databases of the other states for searches. These arrangements were, in principle, extended to all EU member states in 2007, when the Council agreed to integrate the main provisions of the Prüm Treaty into the EU legal framework[823], to enable wider exchanges of biometric data between all EU Member States in the fight against terrorism, illegal migration and cross-border crime.[824] Until 2010, the EU Member States were required to amend domestic laws in order to comply with the EU regulation. Several member states had difficulties in meeting the mid-2011 deadline for the implementation of the provisions on automated data exchange.[825]

Ethical, legal and practical questions arise from the use of DNA profiles for forensic purposes and from the establishment of forensic DNA profile databases. They are:
- coverage of forensic DNA databases, i.e. from whom and under which preconditions samples should be taken and DNA profiles should be stored.
- duration of sample storage and data storage in forensic DNA databases.

---

[819] Genewatch UK, "DNA databases and human rights", Briefing, GeneWatch UK, Buxton, 2011. www.councilforresponsiblegenetics.org/pageDocuments/JZK6YZQS60.pdf.
[820] Interpol DNA Unit, "Global DNA Profiling Survey 2008. Results and Analysis", Interpol, Lyon, 2009.
[821] http://www.dnaforensics.com
[822] Prainsack, Barbara, and R. Hindmarsh, "Beyond borders: trends and challenges in global forensic profiling and databasing", in Prainsack, Barbara, and R. Hindmarsh (eds.), *Genetic Suspects: Global Governance of Forensic DNA Profiling and Databasing*, Cambridge University Press, Cambridge, 2010, pp. 333-341.
[823] Council of the European Union, "Council Decision 2008/616/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime", *Official Journal of the European Union L 210*, 6 August 2008, pp. 12-72. Council of the European Union, "Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime", *Official Journal of the European Union L 210*, 6 August 2008, pp. 1-11.
[824] Stajano, Frank, Lucia Bianchi, Pietro Liò and Douwe Korff, "Forensic genomics: kin privacy, driftnets and other open questions", in Vijay Atluri and Marianne Winslett (eds.), *Proceedings of the 2008 ACM Workshop on Privacy in the Electronic Society, WPES 2008, Alexandria, VA, USA, October 27, 2008*, ACM, New York, 2008, pp. 15-22.
[825] Council of the European Union, "Press release 3043rd Council meeting, Justice and Home Affairs. Brussels, 8 and 9 November 2010", Document No 15848/10, Brussels, 2010.

• purposes and preconditions for accessing and searching forensic DNA databases.

In this context, the function creep is most relevant, i.e. the widening of the scope of purposes for which DNA profiling and databasing are used. This function creep comprises the inclusion of DNA profiles from a wider range of persons, the increasing cross-border use of other national databases for searches, as well as the broadening of kinds of information that can legally be obtained from the analysis of DNA samples (e.g. familial searching).[826]

In general, these questions are often governed by national regulation specific to the national forensic databases. However, out of the 54 countries worldwide with a national DNA database, only 28 countries have implemented database-specific DNA database legislation[827]. Moreover, in international comparison, there is a very wide range of ways in which these questions are solved on a national basis, so that the rules on what data can be collected and stored and how data can be used differ significantly between different countries[828]. For example, with respect to the coverage of forensic DNA databases, the scope ranges from databases in which only DNA profiles of convicted criminals who have committed a severe crime (e. g. murder or rape) are being stored, to countries that plan to set up comprehensive population databases. In countries where DNA profiling is being restricted to severe crimes, the definition of what is being considered "a severe crime" has often been changed to less severe crimes, often triggered by individual cases[829]. Moreover, surveys by data protection officers show deficits in everyday practice in complying with these regulations (e.g. deletion of DNA profiles from the databases of suspects or from mass screenings in a certain investigation once the investigation has been closed and a suspect been convicted). In addition, certain social groups are overrepresented in these databases, pointing to a discriminatory imbalance in the practice of collecting DNA profiles from suspects.

Prospects of whole genome sequencing in forensics

Presently, sequencing of whole individual genomes is not yet done for forensic purposes. However, several drivers can be identified which support an adoption of the techniques in the mid-term[830]:

- New technological solutions to the analysis of mixed DNA samples. A remaining challenge in forensics is the analysis of mixed DNA samples, especially if the different persons whose DNA are mixed in the sample are of the same sex. Experts are of opinion that third generation sequencing of single molecules, without the need for PCR amplification, will help solve this problem. Moreover, if small amounts of degraded DNA have to be analysed, single molecule sequencing may be very useful. Therefore, there is a specific technical need to establish third-generation sequencing technologies in forensic labs. This would also technically allow whole genome sequencing of samples other than the challenging mixed DNA samples.
- Need for new investigational leads. Several technologies and approaches are being explored which bear the potential to open up new investigational leads. Among them are familial searches and DNA-based analytic techniques which allow the inference of phenotypic traits from genetic material. There are policy initiatives, e.g. in the UK, the Netherlands and several US states (Colorado, Florida) to increasingly use familial searches in DNA databases.

[826] Prainsack and Hindmarsh, op. cit, 2010.
[827] Interpol DNA Unit, op. cit., 2009.
[828] Genewatch UK, op. cit., 2011.
[829] Kayser and de Knijff, op. cit., 2011.
[830] Kukk and Hüsing, op. cit., 2011,.

However, these policies are disputed due to unresolved privacy concerns, lack of scientific data and a weak legal framework[831]. Research is underway to use genomic biomarkers, so called single nucleotide polymorphisms (SNPs), instead of or in addition to STRs for forensic purposes. SNPs were – technically speaking – research tools in genomic research that were (and are) widely used before whole genome sequencing became affordable. They are usually tested with DNA arrays, a technology that is also being challenged by next and third-generation DNA sequencing. Provided that more research is carried out, the use of SNPs could allow the inference of genetically determined appearance traits from DNA, such as body height and stature, eye, skin and hair colour, skin pigmentation such as freckles, hair morphology (e.g. woolly hair or male baldness) or cleft lip. Of special interest, but still largely unexplored, are genetic factors that determine facial morphology.[832] To infer such bodily characteristics from crime scene samples could give new and additional clues in investigations. All these traits of interest in criminal investigations could also – or perhaps even better – be analysed with the help of DNA sequencing. Experts are of the opinion that SNP testing will most likely be adopted first in forensics in the identification of disaster victims and in kinship testing once commercial kits become available for these purposes, due to some scientific-technical advantages of SNP testing over STR-based identification in these applications.[833]

However, SNP testing or even whole genome sequencing is incompatible with existing stored DNA profiles based on STRs. This poses a significant hurdle to changing practice in criminal investigations, because it would mean that existing forensic databases would have to be built again from scratch. On the other hand, in countries that have not yet established a forensic database, the use of SNP-based identification or even DNA sequencing could be taken into consideration[834], thus establishing the basis for deducing phenotypic appearance solely from DNA in criminal investigations. As there is a demand for additional technologies and approaches in criminal investigations and whole genome sequencing promises to offer a wealth of such novel approaches, policy makers may also take it into consideration. However, for the time being, it will most likely remain restricted to relatively rare, specific criminal investigations.

6.4 STAKEHOLDERS AND DRIVERS BEHIND THE DEVELOPMENT AND USE OF THE TECHNOLOGY

6.4.1 Industry

Important drivers behind the development are the companies which have developed commercially available sequencing platforms – such as Roche/454 FLX, the Illumina/Solexa Genome analyzer and the Applied Biosystems (ABI) SOLiD Analyzer – that are currently dominating the market. There are also two newcomers, Polonator G.007 and Helicos HeliScope, which have entered the market, but are not that widely used. Because of the increasing speed of technological development, more new technologies are expected to come to the market within the next few years that offer cheaper, faster and more precise sequencing methodologies. There are also some IT companies entering the market. For example, last year IBM announced collaboration project with Roche to develop a nanopore-based technology that will

[831] Gershaw, C. J., A. J. Schweighardt, L. C. Rourke and M. M. Wallace, "Forensic utilization of familial searches in DNA databases", *Forensic Science International: Genetics*, Vol. 5, No. 1, 2011, pp. 16-20.
[832] Kayser and de Knijff, op. cit., 2011.
[833] Ibid.
[834] Ibid.

directly read and sequence human DNA quickly and efficiently. Focused on advancing IBM's recently published "DNA Transistor" technology, the collaboration will take advantage of IBM's leadership in microelectronics, information technology and computational biology and Roche's expertise in medical diagnostics and genome sequencing.[835]

Another important group of companies are providers of kits and consumables for new generation sequencing technologies. Among them are Ambion, Life Technologies, NuGen, Qiagen, Invitrogen, Promega and Sigma Aldrich. The huge amounts of data that have to be processed and stored in whole genome sequencing require a sophisticated IT infrastructure as well as advanced software to analyse the data. Therefore, this field is of interest to both IT hardware and software providers.

Pharmaceutical and diagnostic companies are actively developing drug-diagnostic combinations within the concept of personalised medicine. They apply next-generation sequencing in these efforts and they also make use of the research findings coming from genome sequencing projects.

6.4.2 Stakeholders in research and research policy

Many of innovative approaches to next and third-generation DNA sequencing were initially triggered by National Institutes of Health (NIH) funding through the "Technology development for the $1,000 genome" programme[836] that promised funding support and a $10 million USD award to develop rapid and accurate genomic sequencing technology.[837] As a consequence, research institutes and their spin-off companies are also among the innovators developing new DNA sequencing approaches.

Demand for new DNA sequencing technologies comes from stakeholders in research. They mainly serve as pilot users who team up with leading industrial technology providers for joint development of new technologies, who use the powerful technologies to apply new methodological and conceptual approaches in research and who lend reputation to the newly developed technologies if first results are published in high-ranking scientific journals. They also act as opinion leaders in disseminating the demand for the new technologies.

In basic research, the main funding has come from public sector sources that provide the infrastructure, IT and maintenance costs of biobanks and other basic research costs. Over the last decade, there have been a number of international-scale research projects related to DNA sequencing, all of which have started after the completion of the Human Genome Project in 2001.[838] The HapMap research project aims to map the haplotype diversity in the human genome; the 1000 Genome Project aims to add new information to the understanding of genome diversity by studying more than one thousand genomes; the ENCODE project; etc. Public sector funding for purchase of expensive next and third-generation sequencing equipment and for research projects employing this equipment is associated with the expectations of funding leading-edge research, providing innovative technologies and findings of use for industry, and of contributing to innovation in pharmaceuticals and biomedical research which may translate

[835] IBM and Roche, "Roche and IBM Collaborate to Develop Nanopore-Based DNA Sequencing Technology", Press Release, Yorktown Heights, NY and Branford, Conn., 2010. http://www-03.ibm.com/press/us/en/pressrelease/32037.wss.
[836] http://www.genome.gov/ 11008124#al-4
[837] Mardis, op. cit., 2008,.
[838] Lander, op. cit., 2011.

into improved health care and quality of life. These are expectations that had already been assigned to the Human Genome Project. However, there is controversy over whether the Human Genome Project has lived up to these expectations. The molecular biology research community views genomic and post-genomic information as particularly useful; however, this view is not necessarily shared by researchers with a clinical orientation or medical doctors active in health care.

There are also some private investments. For example, in early spring in 2008 Google announced their decision to invest in world's largest DNA sequencing project "Personal Genome Project". The leader of the project, Harvard's professor George Church is planning to spend nearly $1 billion USD to connect DNA information to each person's health history and create a database to find new medicines.

In medical research, second-generation DNA sequencing technologies have also enabled medical doctors and researchers in university research laboratories and clinical laboratories in university hospitals to investigate disease mechanisms from the DNA sequence to transcriptional regulation and RNA expression.[839]

6.4.3 Health care and direct-to-consumer genetic profiling

Within health care, next-generation sequencing is currently being applied in sequencing a limited number of genes, e.g. in the context of diagnosing hereditary diseases, or in whole exome sequencing in the case of diseases with unexplained causes, such as unexplained mental retardation. The sequencing of tumour DNA in cancer patients is also an upcoming health care application. Relevant actors are human geneticists and oncologists, as well as clinical laboratory services and pathologists.

Although genome-wide screenings are increasingly being advocated by molecular biologists for various groups in the population, a differentiated debate, including clinicians, public health/epidemiology, health policy, is necessary. It should give a realistic assessment whether the promised benefits are likely to be (ever) realised and should discuss how the envisioned practices challenge established ethical and legal norms and principles.

In addition to classical medical and health care players, a new business sector has developed in recent years, which offers direct-to-consumer genetic profiling and whole genome screening to the general public[840]. There are more than 30 companies on the market, mostly SMEs in the USA and Europe. Services are offered mainly over the internet, making them readily available to consumers worldwide. This market has grown steadily over the last 10 years but still lacks steady and established regulatory oversight[841]. Consumers are interested in these services for a variety of reasons, ranging from pure curiosity to the exploration of disease predispositions.[842] However, the number of people actually using genetic profiling services is not

[839] Anderson and Schrijver, op. cit., 2010.
[840] Kukk and Hüsing, op. cit., 2011.
[841] Javitt, Gail, "Which way for genetic-test regulation? Assign regulation appropriate to the level of risk", *Nature*, Vol. 466, No. 7308, 2010, pp. 817-818.
[842] Hogarth, Stuart, Gail Javitt, and David Melzer, "The Current Landscape for Direct-to-Consumer Genetic Testing: Legal, Ethical, and Policy Issues", *Annual Review of Genomics and Human Genetics*, Vol. 9, No. 1, 2008, pp. 161-182. Javitt, op. cit., 2010. Hennen, Leonhard, Arnold Sauter, and E. van den Cruyce, "Direct to consumer genetic testing", Final Report IP/A/STOA/FWC/2005-28/SC 39, European Parliament, DG Internal Policies, Policy Department A: Economic and Scientific Policy, STOA, Brussels, 2008.

known.[843] Software companies such as Microsoft and Google significantly invest in and co-operate with DTC genetic profiling companies, such as 23andMe and Navigenics[844], located in the USA. For example, in 2009 Google invested $4.4 million USD in these two companies.

6.4.4 Forensics

Since the mid-1990s most EU Member States have established a national forensic DNA database for public security reasons. These mass repositories of DNA profiles enable the police and immigration officers to identify DNA stains which are found at crime scenes or are collected for immigration issues.[845] Currently, DNA profile testing by police agencies is often outsourced, e.g. to academic forensic institutes, for various reasons, such as a need for additional man power or the occasional crime scene that presents evidence that is especially challenging to collect and process.

As an international police organisation, INTERPOL advocates the international comparison of DNA profiles in accordance with international standards, to combat cross-border crime and criminals.[846] There is an increasing interlinking of forensic databases across borders, as can be seen from the Prüm Treaty.

6.5 PRIVACY IMPACTS AND ETHICAL ISSUES RAISED BY THE WHOLE DNA SEQUENCING TECHNOLOGY

Genetic information is personal, sensitive information that has a unique combination of specific features which are of relevance to data protection and privacy. In the following paragraphs, we will first outline these characteristics, followed by an overview of possible privacy infringements and concerns that are associated with whole genome sequencing and analysis.

6.5.1 Features of genomic information

Genomic information can be characterised by the unique combination of the following features:[847]

- Identifying. Each individual has a unique genomic sequence. Therefore, the whole genome sequence could act like a unique bar code to identify individuals. Because persons inherit half their DNA from their mother and half from their father, DNA sequence information can also be used to identify their relatives. Close relatives have a DNA sequence that is more alike than distant relatives or than someone who is unrelated.[848] Once the full genomic sequence is known, it is impossible to de-identify or anonymise the DNA sample or the DNA sequence.
- Diagnosis of genetic diseases. Approximately 3,000 diseases are known to be caused by mutations in a single gene or a small number of genes (although the causative genes may still be unknown). DNA sequencing can show whether the gene is mutated or not. DNA sequencing can therefore be used for diagnosis when clinical symptoms are evident, but also

[843] Weale, et al., op. cit., 2010.
[844] Pray, Leslie, "DTC Genetic Testing: 23andme, DNA Direct and Genelex", *Nature Education*, Vol. 1, No. 1, 2008, pp. http://www.nature.com/scitable/topicpage/DTC-Genetic-Testing-23andme-DNA-Direct-and-674.
[845] Van Camp, N., and K. Dierickx, "The retention of forensic DNA samples: a socio-ethical evaluation of current practices in the EU", *Journal of Medical Ethics*, Vol. 34, No. 8, 2008, pp. 606-610.
[846] Interpol DNA Unit, op. cit., 2009.
[847] Kukk and Hüsing, op. cit., 2011.
[848] Genewatch UK, op. cit., 2011.

before symptoms occur (predictive). Moreover, heterozygous carriers of this mutation, who will not become ill themselves but may transfer the mutation to their offspring, can be identified.

- Prediction of predispositions. Many multifactorial diseases and complex non-health related traits, such as behaviour, cognition and personality, have a genetic component, but other factors also contribute. DNA sequencing can be used to identify and characterise the genetic portion of the trait. If the genetic component can be determined, a certain predisposition can be stated, but it is a question of probabilities rather than certainties whether the trait or disease will develop in the "predicted" way in the individual.
- Individual and familial nature of genetic information, shared information. Due to the hereditary nature of genetic information, most genetic information flows between generations. Therefore, the abovementioned implications do not only apply to the individual from whom the DNA was taken and analysed, but it may extend to the family and beyond to larger groups of people linked by common ancestry. In a clinical setting, genetic information may reveal that individuals as well as family members may be affected by a disease or predisposition to a disease, challenging individual autonomy and consent as well as the duty to warn and the right not to know. If a particular genetic condition is prevalent in a specific subpopulation, harm may arise for those who are part of this population.
- Risk of discrimination and stigmatisation. Genetic information may put individuals, families and communities at risk of discrimination and stigmatisation due to their genetic condition, especially if they are not (and may never become) ill, but are still predisposed to disease or are asymptomatic heterozygous carriers.
- Availability. DNA is contained in every human cell. Certain types of DNA analysis can be done from picogram amounts of human DNA available from a few dozens of human cells, which can be taken from, for example, blood, hair roots, oral mucosa cells in saliva, or skin. Therefore, it is possible to take and analyse a person's DNA without their knowledge or consent, simply by collecting cells that are both unintentionally and unavoidably left behind.
- Long-term availability. If stored properly, DNA-containing biological samples and isolated DNA are available for indeterminate periods of time. Techniques are available to amplify the DNA. Samples taken once can therefore be amplified and re-analysed repeatedly, e.g. as technology and scientific understanding develops.
- Availability before birth and after death. Most of the genetic information of a person remains constant over lifetime. It can be analysed whenever DNA-containing biological material from this person can be made available. Therefore, genetic information can already be obtained before birth (e.g. during prenatal genetic testing or pre-implantation screening) or after death (even decades to centuries after death, depending on the preservation of the biological material).
- Symbolic meaning. Genetic information is socially often perceived as a blueprint representing the essence of human life and as such has a symbolic quality.

6.5.2 Overview of data protection issues and possible privacy infringements

It is obvious that whole genome sequencing will yield a wealth of personal, sensitive data which do not only relate to the donor of the genomic DNA, but also their relatives. The following data protection issues and privacy infringement concerns have been voiced[849]:

[849] Stajano, et al., op. cit.,2008. "Editorial: DNA confidential", *Nature Biotechnology*, Vol. 27, No. 9, 2009, pp. 777. Lunshof, et al., op .cit., 2010. Wjst, Matthias, "Caught you: threats to confidentiality due to the public release of large-scale genetic data sets", *BMC Medical Ethics*, Vol. 11, No. 1, 2010, pp. 21. Heeney, et al., op. cit., 2011. Kukk and Hüsing, op. cit., 2011 .

- The disclosure of genomic information to the public or to third parties, with the risk of unintended and harmful use of this information;
- Use of genomic data to identify the DNA donor in other confidential settings (e.g. research studies, health care, criminal investigations);
- Use of disclosed genomic information without knowledge or consent by the donor to
  - infer paternity or other features of the donor's genealogy;
  - reveal the possibility of a disease or unknown propensity for a disease or carrier status for a genetic disease, thus also influencing reproductive choices;
  - reveal non-medical traits with a genetic basis, such as aberrant behaviour, sexual orientation, intelligence and so on;
  - use genetic information to infer phenotypic traits, e.g. facial morphology, skin, eye and hair colour, stature and so on, thus identifying the DNA donor or a relative, e.g. in a confidential setting or for biosurveillance purposes;
  - claim statistical evidence that could affect employment, insurance or ability to obtain financial services;
  - claim a relation to criminals, criminal suspects or involvement in crimes;
  - make synthetic DNA and use it for identity theft, to falsely identify the DNA donor or, to put the synthetic DNA at a crime scene;
- Attempted or actual stigmatisation, discrimination and other forms of negative treatment due to disclosure of personal genomic information or its interpretation, in the context of education, employment, insurance, health care services, financial services, social contacts, criminal investigations and so on.

The related privacy concerns and ethical issues of whole genome analysis show a broad overlap with well-known and elaborated privacy concerns and ethical issues concerning genetic testing for research and medical purposes, genetic profiling for forensic purposes, and privacy issues of medical information. However, the following combination of features is new and specific for whole genome sequencing:[850]

- The sheer amount and comprehensiveness of information made accessible by whole genome sequencing and analysis. It goes far beyond single gene information or simple identification (as through DNA profiles). Information about medical conditions, non-medical traits and ancestry may be retrieved. It significantly increases the possibilities and likelihood of unintended use or misuse of the data with respect to discrimination, stigmatisation and privacy infringements. It implies an urgent need for (even more) stringent safeguards for data protection and confidentiality and against unauthorised use of data. It also impacts established procedures for obtaining informed consent and raises ethical issues.
- The difficulty or even impossibility to apply established safeguards for privacy, such as confidentiality or anonymisation, of whole genome data[851].
- The tentativeness of the results of whole genome analysis, due to incomplete knowledge at the time of consent or analysis, and the highly possible option that future re-analyses of the sequence data will reveal additional information not foreseeable at the time of DNA sequencing. This opens up new possibilities of unintended or abusive analysis of personal genome data, and it also impacts established procedures for obtaining informed consent and requires ethical deliberations.
- The change of contexts (players, codes of conduct) in which whole genome sequencing and whole genome analysis is being performed, as compared to genetic testing, genetic research

[850] Kukk and Hüsing, op. cit., 2011.
[851] Curren, Liam, Paula Boddington, Heather Gowans, et al., "Identifiability, Genomics and UK Data Protection Law", *European Journal of Health Law*, Vol. 17, No. 4, 2010, pp. 329-344. Wjst, op. cit., 2010.

and health care. This relates mainly to the need to amend and adapt established governance models such as codes of conduct or sector-specific regulations to the new requirements.
- An increasing internationalisation and DNA and data exchange across borders in research, health care and criminal investigations, but with different levels of national safeguards and regulations in place, and a lack of harmonisation of these regulations. This increases the possibility of unintended uses and privacy infringements when personal genome data or genomic DNA crosses borders.

6.5.3 Privacy issues in research

Traditionally, legal frameworks have sought to balance the privacy of data subjects with the benefits of research by relying heavily on informed consent and anonymisation[852], meaning that the protection of the identity of participants in research projects is guaranteed by the maintenance of the confidentiality of health information through mechanisms such as only releasing data in an aggregated form or after identifying variables have been removed.[853] Also, the current framework for protecting informational privacy assumes that the use of genomic datasets, or at least the resources to make use of them, would largely be restricted to the scientific research community; however, in an internationally cooperating research community which also interacts closely with industry this is not always true anymore.[854] Although technical and organisational measures are being implemented to ensure data protection, both the structures in which whole genome sequencing research takes place, as well as the enormous amount of personal, sensitive information generated and processed, increase the likelihood that research participants' identities could be inferred and genomic data be accessed in an unauthorised way.[855]

Against this background there is a need to adapt and modernise established practices and rules, with respect to the following questions:
- What level of confidentiality and data protection can realistically be promised to research subjects[856]?
- What information has to be given within the process of informed consent, given
  - the uncertainty of future research uses,
  - the uncertainty of future analysis of personal data[857],
  - that different types of players may or should gain access to data in the future,
  - Are there new ways of benefit sharing between researcher and participant? What research findings should be revealed to the participants, in what form and by what procedure?

The Personal Genome Project is an illustrative example for research projects that aim at elucidating the relationship between genetic condition, environmental influences and health by collecting the most comprehensive molecular information (e.g. whole genome sequence, transcriptome, proteome and metabolome data), as well as whole body imaging and comprehensive health and lifestyle information from healthy volunteers. A key feature of the Personal Genome Project is that is does not guarantee anonymity, privacy and confidentiality for the

[852] Lunshof, et al., op. cit., 2008.
[853] Heeney, et al., op. cit., 2011.
[854] Curren, et al., op. cit., 2010.
[855] Ibid.
[856] Greenbaum, D., J. Du and M. Gerstein, "Genomic Anonymity: Have We Already Lost It?", *American Journal of Bioethics*, Vol. 8, No. 10, 2008, pp. 71-74.
[857] Tavani, H. T., "Genomic research and data-mining technology: implications for personal privacy and informed consent", *Ethics and information technology.*, Vol. 6, No. 1, 2004, pp. 15-28.

participants. Rather, volunteers are urged to seriously consider the scenario where all of their data and identity would be accessible by a large number of people. As a consequence and novelty in research ethics, the concept of "open consent" was developed.[858] It is put into practice by comprehensive information for the volunteers, an entrance exam to test their knowledge and understanding of what their consent really means, and an eligibility screening. For these purposes, a number of project specific tools and resources have been developed.[859] In the Personal Genome Project, open research is advocated as one possible solution to the question whether and how research results should be reported back to the participants. Open research implies veracity on the part of the researchers, active and interactive modes of participation, and openness from both researchers and participants.[860] However, the communitarian position that is reflected in the setup of the Personal Genome Project is controversially debated, as it ranks moral obligation to contribute to collective interests (e.g. research), solidarity, reciprocity and citizenship much higher than autonomy and privacy of the individual.

6.5.4 Health care and direct-to-consumer genomic profiling

Whole genome sequencing in a health care setting will inevitably create significantly more information than is required for answering the initial clinical question (e.g. diagnosis, risk specification). Therefore, the majority of findings will be unsought for, or incidental, findings, which will be generated at a much higher probability.[861]

Based on the both the right to know and the right not to know, the established ethical framework for such diagnostic and screening purposes means that people should be given the opportunity to make fully informed choices in advance. Against this background, guidelines and quality standards have been implemented concerning how genetic counselling should be performed for diagnostic genetic testing, in order to obtain valid, informed consent. It comprises a detailed discussion of all possible findings with respect to the nature, severity and treatability of potential issues. However, it will be impossible to apply this standard in whole genome sequencing and analysis because of the amount and variety of the information, as well as the fact that a great deal remains unclear or uncertain.[862] As a possible solution, a "generic consent" model has been proposed. In this model, a selection of typical examples of diseases and possible results are explained to the patient or participant, and consent is sought on the basis of these exemplary explanations.[863] Moreover, the following options must also become an integral part of the consent process: to what extent should raw sequencing data be stored, under what conditions should the raw data be accessed and analysed again, and to what extent should unclear or health information from analysis be disclosed to the patient? Expert discourses as well as public consultations will have to be initiated in the mid-term in order to assess risks and possible benefits from genome-wide screenings, especially if neonates or children should be screened. In this context, the issue of unsought-for findings which will be produced at unprecedented scale by whole genome sequencing must also be addressed in an interdisciplinary manner.[864]

[858] Lunshof, et al., op. cit., 2008..
[859] Lunshof, et al., op. cit., 2010.
[860] Lunshof, et al., op. cit., 2008.
[861] Health Council of the Netherlands, et al., op. cit., 2010.
[862] Ibid.
[863] Kukk and Hüsing, op. cit., 2011.
[864] Ibid.

In the case of direct-to-consumer genomic profiling, services are provided without the involvement of a health care provider, on a private contractual, commercial basis. As a consequence, the principle of confidentiality, as firmly established in the doctor-patient relationship, no longer applies in the case of DTC genomic profiling companies as new actors.[865] There is an on-going debate about whether and how the new situation should be dealt with, especially as the number of persons using these services or any harms they have experienced are not known. On the one hand, there are voices that advocate a ban of direct-to-consumer medical tests, thus leaving the analysis of clinical diagnostics to specialists.[866] On the other hand, others call for new governing models, not just an extension of existing regulations[867]. The UK Nuffield Council on Bioethics takes a liberal position with respect to DTC genetic profiling, by concluding and recommending the following:

- Regulators should request evidence for any claims being made by companies about the clinical value of their tests.
- Government websites should provide information about the risks and benefits of personal genetic profiling, including the relevance for insurance.
- Companies should not knowingly analyse the DNA of children unless certain criteria are met.
- Doctors should receive training on giving advice to patients about commercial genetic profiling services.
- Companies should voluntarily provide clear information on the limitations of genetic profiling and what will happen to people's data.[868]

6.5.5 Privacy issues in forensics

Use of genomic data in criminal investigations bears the potential to intrude into bodily integrity and challenge civil liberties and legal principles, such as the presumption of innocence, proportionality of measures, the right not to know and the burden of proof.

Presently, only forensic DNA profiling is being used, and the sequencing of whole genomes for forensic purposes is unlikely to be implemented in the mid-term beyond rare, specific criminal investigations. However, in an international perspective, ethical, legal and practical questions when using DNA profiles for forensic purposes are not yet sufficiently dealt with and there are several weaknesses in the existing regulations and their enforcement in practice:[869]

- The level of awareness and reflection of these issues differs strongly between states;
- Many countries lack specific regulations governing these issues: in international comparison, the regulatory landscape is not only patchy, but also diverse and non-harmonised;
- In countries where specific regulations exist, there may be difficulties and shortcomings in implementing these regulations; cases of non-compliance with existing regulations have been reported.
- High quality standards need to be implemented to prevent any miscarriages of justice due to errors in DNA profiling. This becomes even more pressing by international linking of foren-

[865] Hogarth, Stuart, Gail Javitt, and David Melzer, "The Current Landscape for Direct-to-Consumer Genetic Testing: Legal, Ethical, and Policy Issues", *Annual Review of Genomics and Human Genetics*, Vol. 9, No. 1, 2008, pp. 161-182.
[866] Beaudet, Arthur L., "Which way for genetic-test regulation? Leave test interpretation to specialists", *Nature*, Vol. 466, No. 7308, 2010, pp. 816-817.
[867] Prainsack, Barbara, Jenny Reardon, Richard Hindmarsh et al., "Personal genomes: Misdirected precaution", ibid.Vol. 456, No. 2008, pp. 34-35.
[868] Weale, et al., op. cit., 2010.
[869] Kukk and Hüsing, op. cit., 2011.

sic databases, since the probability of errors occuring is increased with the number of profiles and comparisons.

As a consequence, the current situation with DNA profiling needs to be improved. Existing problems with DNA profiles will become even more relevant in the mid-term should whole genome sequencing and whole genome analyses be introduced into forensics.

6.6 EXTENT TO WHICH THE EXISTING LEGAL FRAMEWORK ADDRESSES THE PRIVACY IMPACTS

There is an on-going debate about whether genetic information, due to the unique combination of the features outlined in section 6.5.1, is exceptional, and therefore requires a special regulatory framework to prevent threats to privacy and misuse, or, whether despite its sensitive nature, genetic information can be adequately protected under regimes that currently regulate personal data or other medical and health information. The assumption of an exceptional character of genetic information is an integral principle underlying major regulations. Several international instruments already prohibit any discrimination based on genetic data, like Council of Europe's European Convention on Bio-medicine, Article 11; EU's Charter of Fundamental Rights, Article 21 and UNESCO's "Universal Declaration on Human Genome and Human Rights", Article 6. The Convention on Human Rights and Biomedicine (the Oviedo Convention) furthermore allows the carrying out of predictive genetic tests for medical purposes only.

The US Genetic Information Non-Discrimination Act (GINA) was signed into law on 21 May 2008. GINA provides protection from discrimination based on pre-symptomatic genetic information in health insurance and in the workplace, and creates a national uniform standard ensuring that Americans will receive the same minimum protections.

Data protection law in Europe also requires strong protection of genetic data, as emphasised by the EU's "Article 29 Working Party" in its 2004 Working Document on Genetic Data.[870] However, as some authors point out, in many respects the Art. 29 WP only identifies issues and questions, without providing conclusive answers.[871] Examples include the question of whether a person may be forced to disclose his/her genetic data to blood relatives, where such data are relevant in view of safeguarding their health; the exercise of the right, inside a group, not to know one's genetic data; and in respect to biobanks, that "the issue of prescribing practices applying anonymisation could be a possibility to address issues from the data protection perspective".[872] However, the Art. 29 WP also noted that "there has been evidence that stored DNA is capable of being linked to a particular person – provided certain additional knowledge is available, even though it may not be stored in a directly person-specific way".[873]

Moreover, the EU's data protection directive (Directive 95/46/EC), that is based on the 1980 OECD "Recommendations of the Council Concerning guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data", is already enforced in the majority of EU Member States[874].

[870] Article 29 Data Protection Working Party, "Working Document on Genetic Data", 12178/03/EN, WP 91, Brussels, 2004.
[871] Stajano, et al., op. cit., 2008.
[872] Article 29 Data Protection Working Party, op. cit., 2004.
[873] Ibid.
[874] Stajano, et al., op. cit., 2008.

6.6.1 Current regulations in forensics

There is an agreement in place ("Prüm Treaty") since 2005 when Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria all agreed that nationally collected DNA profiles, fingerprint data and vehicle data should be searchable by the other countries. It covers a series of justice and home affairs issues including the "exchange of information", and allows the police forces of their countries to compare and exchange data more easily. The treaty, adopted by the European Parliament's report of Fausto Correia and approved by the Council of Ministers during a meeting of the justice and home office ministers in June 2007[875], gave EU Member States three years (until mid-2010) to rewrite domestic laws and integrate the main provisions of the Prüm Convention into the EU's legal framework, to enable wider exchanges between all EU Member States of biometric data (DNA and fingerprints) in the fight against terrorism and cross-border crime. All EU Member States were therefore required to set up DNA databases.[876]

This agreement meant that other EU police forces will be allowed to search national databases for people suspected of committing a crime abroad. In June 2007, the EU adopted its own data exchange law, which was very similar to the original Prüm Treaty. The new law, approved by the Council of Ministers during a meeting of the justice and home office ministers, gave the EU Member States three years to rewrite domestic laws in order to comply. Unfortunately, some states continue to fail to comply.[877] Also, out of the 27 Member Countries of the European Union, many countries have failed to pass any forensic DNA database legislation. Out of the 54 countries worldwide with a national DNA database, 28 countries have implemented database-specific DNA database legislation.[878] However, rules on what data can be collected and stored and how it can be used differ greatly between different countries[879]. Some of those databases (e.g. UK Police National DNA Database) have been criticised on privacy grounds.[880]

6.7 CONCLUSIONS

Whole genome sequencing and its related data protection and privacy concerns are most relevant in research and health care. In these fields of application, whole genome sequencing is either already in active use, or will be adopted in the coming five to ten years, thus putting existing governance principles and practices for ensuring privacy under pressure.

As outlined in section 6.4, high-end DNA sequencing technologies and their use in research and health care are being initiated and supported by publicly funded research, with industry and researchers presently being the major beneficiaries. The rationale is the contribution to

[875] "The Integration of the "Prüm Treaty" into EU-legislation - Council decision on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime", Press Release IP/07/803, Brussels, 2007.
[876] Stajano, et al., op. cit., 2008.
[877] Council of the European Union, "Council Decision 2008/616/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime", *Official Journal of the European Union L 210*, 6 August 2008, pp. 12-72. Council of the European Union, "Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime", *Official Journal of the European Union L 210*, 6 August 2008, pp. 1-11.
[878] Interpol DNA Unit, op. cit., 2009.
[879] Genewatch UK, op. cit., 2011.
[880] Staley, Kristina, "The police National DNA Database: balancing crime detection,human rights and privacy", GeneWatch UK, Buxton 2011.

public goods such as scientific knowledge, innovation, international competitiveness as well as individual and public health. However, in democratic societies, certain guarantees for individual privacy are a public good as well, so that the challenge with whole genome sequencing is the balancing of these partly competing public goods.

In forensic applications, especially criminal investigations, the challenge posed by whole genome sequencing seems to be less urgent. Although we could identify drivers and demands which may act synergistically to acquire the technologies and competencies to carry out whole genome sequencing and analysis and to infer new investigational leads (e.g. phenotypic traits) from genetic material, it is unlikely that whole genome sequencing will be carried out beyond rare, specific criminal investigations in the foreseeable future. The sunk investment in forensic databases, based on DNA profiles, poses a significant hurdle to switch to whole genome sequencing in the near term. However, data protection and privacy are already challenged by DNA profiles, pointing to the need to

- implement specific national regulations governing forensic DNA profiling and databasing for forensic purposes in the currently patchy and non-harmonised regulatory landscape. Moreover, international harmonisation and implementation of international standards should be strived for, especially as cross-border searches of national databases are increasing.
- implement high quality standards and stricter monitoring of DNA profiling and databasing practices, in order to reduce breaches of privacy regulations and to prevent miscarriages of justice due to errors in DNA profiling.
- initiate and support an increase in transparency and a broad debate about DNA profiling, databasing and – in perspective – also whole genome sequencing for forensic purposes. These debates should address scientific soundness, governance and oversight and must not stay confined to professional experts; they should also seek civic engagement.

Genomic information is personal, sensitive information. While data protection issues are most relevant for the generation of DNA sequence data, its storage, data exchange and access to these (raw or processed) data, privacy concerns are mainly linked to those pieces of information that are inferred from the raw data sequences after their processing by analytical algorithms which assign functions and traits to the raw sequence data.

Established data protection principles comprise both purpose and data quality principles, resulting in data minimisation principles. All these principles are challenged by whole sequencing:

The purpose specification principle requires that data are collected for specified, explicit and legitimate purposes. With whole genome sequencing, we observe the trend to broaden purposes and to make them less specific: in research, data are increasingly being collected for "general research purposes", which also includes future, not yet specifiable research questions and often includes data sharing "by default", which may include actual or future, not yet specified co-operations across institutions, sectors (academic/public – private) and borders. In health care, genetic testing usually is performed with the purpose of diagnosing (or excluding) a suspected disease or establishing carrier status for a suspected disease. Genome-wide diagnostic and screening procedures, however, would mean the screening not for a single, but for a large number, of conditions or even for unspecified or unknown conditions.

Data protection principles require that data collected for one purpose may only be used for other purposes under certain circumstances. In the case of whole genome sequencing, this could, for example, mean that whole genome data would be collected in health care, but used in research, or were collected in research, but would also be used for criminal investigations. For this case study, we have no information available about whether this is a relevant problem or whether there is merely the potential for violation of the purpose specification principle. Nevertheless, specific regulations would be required which exclude the use of data for certain other purposes or specify the circumstances and preconditions under which this should be possible. However, such regulations, e.g. research biobank laws, forensic database laws, are largely lacking in EU member states, and are not harmonised.

Data protection principles also require that data storage time should only be as long as needed for the purpose. Again, we observe a tendency for storage times to become longer, as purposes becomes less specified, so that it becomes more difficult to define clear end points.

It is an inherent characteristic of whole genome sequencing that an excess of data is collected. This challenges the data quality and data minimisation principles that only data relevant and not excessive in relation to the purpose must be collected. Rather, a "data maximisation principle" often seems to be advocated or even followed. Such a "data maximisation concept" is the basis of many large-scale research projects, e.g. the Personal Genome Project. While in research this data maximisation principle may be justified by the research purpose to elucidate which information is really required for a certain purpose, the challenge to the data minimisation principle becomes more relevant in health care. Here, genome-wide approaches would significantly increase the probability of unsought-for findings and of findings which clinical relevance is uncertain or unknown. By contrast, in evidence-based medicine it is established clinical practice that decision making in health care is based on reductionist models that need to be populated only with relevant (and validated, evidence-based) data. Against this background, information overflow and irrelevant data create more problems than they solve. However, this view is presently neglected in research, and there is an urgent need to stress this aspect if research findings from whole genome approaches are to be translated into the clinic. Therefore, there will be a growing need for either purpose-specific filters for analysing raw data; or purpose-specific sequencing of small, specific parts of the genome.

Another aspect of data protection is that an anonymisation of data for whole or extensive data sets is not possible, since the whole genome sequence is a unique identifier for individuals, and also, with certain probabilities, for relatives. From the point of view of data protection and privacy, this points to the need for strict controls over access to whole data sets.

So what are the policy options? With respect to data protection, whole DNA sequencing, due to the excess of data generated and its personal and sensitive nature, calls for highest standards in data protection, comprising technical measures, organisational measures (e.g. access restrictions, access only to partial data, and anonymisation of partial data), and a strict monitoring of whether these standards are being complied with. It would be highly desirable to support this with a much more intensive, conceptual discussion of how to operationalise the data protection principles for whole genome sequencing.

Privacy protection issues are primarily relevant in the analysis and interpretation of raw sequence data. As privacy aims at protecting the autonomy and self-determination of each individual, consent is of crucial importance. The analysis in section 6.5 showed that concepts of narrow informed consent are increasingly being replaced by generic or even open consent

concepts, leading to the questions how meaningful, valid and informed such consent can be, and whether open, participatory research and information on research results, as advocated in the Personal Genome Project, can be considered as ethical and as a sufficient incentive and fair exchange for giving away control over personal sensitive data that is being processed by third parties?

To sum up, there is a need[881]

- To raise the awareness of the data protection and privacy issues and challenges of whole genome sequencing.
- To actively initiate and support a broad debate about whole genome sequencing for different purposes, which must not stay confined to professional experts, but should also seek civic engagement. Such broader discussions will also contribute to enhancing public trust in research, medical and forensic practices, if a (national) consensus can be achieved on how a fair balance can be struck between competing public goods of knowledge generation through research, high quality health care, efficient criminal investigation and individual civil rights and liberties.
- To implement high quality standards and stricter compliance monitoring of genome-wide approaches and databasing practices in research, health care and forensics.
- To implement specific national regulations (also) governing whole genome sequencing and databasing in the context of research, biobanks, health care and criminal investigations. These national regulations should take the nationally established practices and understandings of "how things are done" into account and be based on the general concepts and values of the social order in the respective country. In addition, an international harmonisation and implementation of international regulations at the EU level should be strived for.

6.8 REFERENCES

Anderson, Matthew W., and Iris Schrijver, "Next Generation DNA Sequencing and the Future of Genomic Medicine", *Genes*, Vol. 1, No. 1, 2010, pp. 38-69.

Article 29 Data Protection Working Party, "Working Document on Genetic Data", 12178/03/EN, WP 91, Brussels, 2004.

Babiel, Rainer, "Personal communication during the workshop 'Privacy issues arising from next generation whole genome sequencing'", Brussels, 1 June 2011.

Beaudet, Arthur L., "Which way for genetic-test regulation? Leave test interpretation to specialists", *Nature*, Vol. 466, No. 7308, 2010, pp. 816-817.

Branton, D., D. W. Deamer, A. Marziali, et al., "The potential and challenges of nanopore sequencing", *Nature Biotechnology*, Vol. 26, No. 10, 2008, pp. 1146-1153.

Check Hayden, Erika, "Genomics shifts focus to rare diseases", *Nature*, Vol. 461, No. 7263, 2009, pp. 458-459.

Council of the European Union, "Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime", *Official Journal of the European Union*, L 210, 6 August 2008, pp. 1-11.

[881] Kukk and Hüsing, op. cit., 2011.

Council of the European Union, "Council Decision 2008/616/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime", *Official Journal of the European Union*, L 210, 6 August 2008, pp. 12-72.

Council of the European Union, "Press release 3043rd Council meeting, Justice and Home Affairs. Brussels, 8 and 9 November 2010", Document No 15848/10, Brussels, 2010.

Curren, Liam, Paula Boddington, Heather Gowans, et al., "Identifiability, Genomics and UK Data Protection Law", *European Journal of Health Law*, Vol. 17, No. 4, 2010, pp. 329-344.

Drmanac, R., A. B. Sparks, M. J. Callow, et al., "Human Genome Sequencing Using Unchained Base Reads on Self-Assembling DNA Nanoarrays", *Science*, Vol. 327, No. 5961, 2010, pp. 78-81.

"Editorial: DNA confidential", *Nature Biotechnology*, Vol. 27, No. 9, 2009, pp. 777.

Gail, J., "Which way for genetic-test regulation? Assign regulation appropriate to the level of risk", *Nature*, Vol. 466, No. 7308, 2010, pp. 817-818.

Genewatch UK, "DNA databases and human rights", Briefing, GeneWatch UK, Buxton, 2011. www.councilforresponsiblegenetics.org/pageDocuments/JZK6YZQS60.pdf.

Gershaw, C. J., A. J. Schweighardt, L. C. Rourke, and M. M. Wallace, "Forensic utilization of familial searches in DNA databases", *Forensic Science International: Genetics*, Vol. 5, No. 1, 2011, pp. 16-20.

Go, A. T. J. I. , J. M. G. van Vugt and C. B. M. Oudejans, "Non-invasive aneuploidy detection using free fetal DNA and RNA in maternal plasma: recent progress and future possibilities", *Human Reproduction Update*, Vol. 17, No. 3, 2011, pp. 372-382.

Greely, Henry T., "Get ready for the flood of fetal gene screening", *Nature*, Vol. 469, No. 7330, 2011, pp. 289-291.

Greenbaum, D., J. Du and M. Gerstein, "Genomic Anonymity: Have We Already Lost It?", *American Journal of Bioethics*, Vol. 8, No. 10, 2008, pp. 71-74.

Harper, J.C., E. Coonen, M. De Rycke, et al., "ESHRE PGD consortium data collection X: cycles from January to December 2007 with pregnancy follow-up to October 2008", *Human Reproduction Update*, Vol. 25, No. 11, 2010, pp. 2685-2707.

Health Council of the Netherlands, Wybo J. Dondorp, and Guido M.W.R. de Wert, "The 'thousand-dollar genome': an ethical exploration", Monitoring Report Ethics and Health 2010/2, Centre for Ethics and Health, The Hague, 2010. http://www.gezondheidsraad.nl/en/publications/thousand-dollar-genome-ethical-exploration.

Heeney, Catherine, N. Hawkins, J. de Vries, et al., "Assessing the Privacy Risks of Data Sharing in Genomics", *Public Health Genomics*, Vol. 14, No. 1, 2011, pp. 17-25.

Hennen, Leonhard, Arnold Sauter, and E. van den Cruyce, "Direct to consumer genetic testing", Final Report IP/A/STOA/FWC/2005-28/SC 39, European Parliament, DG Internal Policies, Policy Department A: Economic and Scientific Policy, STOA, Brussels, 2008.

Hogarth, Stuart, Gail Javitt and David Melzer, "The Current Landscape for Direct-to-Consumer Genetic Testing: Legal, Ethical, and Policy Issues", *Annual Review of Genomics and Human Genetics*, Vol. 9, No. 1, 2008, pp. 161-182.

Howard, H.C., D. Avard and P. Borry, "Are the kids really all right? Direct-to-consumer genetic testing in children: are company policies clashing with professional norms?", *European Journal of Human Genetics*, Vol. 19, No. 11, 2011, pp. 1122-1126.

Hüsing, Bärbel, Juliane Hartig, Bernhard Bührlen, et al., "Individualisierte Medizin und Gesundheitssystem. Zukunftsreport", TAB-Arbeitsbericht 126, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Berlin, 2009.

IBM and Roche, "Roche and IBM Collaborate to Develop Nanopore-Based DNA Sequencing Technology", Press Release, Yorktown Heights, NY and Branford, Conn., 2010. http://www-03.ibm.com/press/us/en/pressrelease/32037.wss.

"The Integration of the "Prüm Treaty" into EU-legislation - Council decision on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime", Press Release IP/07/803, Brussels, 2007.

Interpol DNA Unit, "Global DNA Profiling Survey 2008. Results and Analysis", Interpol, Lyon, 2009.

Javitt, G., "Which way for genetic-test regulation? Assign regulation appropriate to the level of risk", *Nature*, Vol. 466, No. 7308, 2010, pp. 817-818.

Jeffreys, A.J., V. Wilson, and S.L. Thein, "Individual-specific 'fingerprints' of human DNA", *Nature*, Vol. 316, No. 6023, 1985, pp. 76-79.

Jobling, M.A., and P. Gill, "Encoded evidence: DNA in forensic analysis", *Nature Reviews Genetics*, Vol. 5, No. 10, 2004, pp. 739-751.

Kaye, J., "The regulation of direct-to-consumer genetic tests", *Human Molecular Genetics*, Vol. 17, No. 2008, pp. R180-R183.

Kayser, M., and P. de Knijff, "Improving human forensics through advances in genetics, genomics and molecular biology", *Nature Reviews Genetics*, Vol. 12, No. 3, 2011, pp. 179-192.

Kircher, M., and J. Kelso, "High-throughput DNA sequencing - concepts and limitations", *Bioessays*, Vol. 32, No. 6, 2010, pp. 524-536.

Koboldt, D. C., L. Ding, E. R. Mardis and R. K. Wilson, "Challenges of sequencing human genomes", *Briefings in Bioinformatics*, Vol. 11, No. 5, 2010, pp. 484-498.

Kukk, Piret, and Bärbel Hüsing, "Privacy, data protection and policy implications in whole genome sequencing", in van Est, Rinie, and Dirk Stemerding (eds.), *Making Perfect Life. Bio-engineering (in) the 21st Century*. Deliverable No. 5 of the STOA Project "Making Perfect Life", Rathenau Institute, The Hague, 2011, pp. 37-70.

Lander, E. S., "Initial impact of the sequencing of the human genome", *Nature*, Vol. 470, No. 7333, 2011, pp. 187-197.

Lunshof, Jeantine E., Ruth Chadwick, Daniel B. Vorhaus and George M. Church, "From genetic privacy to open consent", *Nature Reviews Genetics*, Vol. 9, No. 2008, pp. 406-411.

Lunshof, Jeantine E., Jason Bobe, John Aach, et al., "Personal genomes in progress: from the human genome project to the personal genome project", *Dialogues in Clinical Neuroscience*, Vol. 12, No. 1, 2010, pp. 47-60.

Mardis, E. R., "The impact of next-generation sequencing technology on genetics", *Trends in Genetics*, Vol. 24, No. 3, 2008, pp. 133-141.

Mardis, E. R., "A decade's perspective on DNA sequencing technology", *Nature*, Vol. 470, No. 7333, 2011, pp. 198-203.

Mastenbroek, S., M. Twisk, F. van der Veen and S. Repping, "Preimplantation genetic screening: A systematic review and meta-analysis of RCTs", *Human Reproduction Update*, Vol. 17, No. 4, 2011, pp. 454-466.

Najmabadi, H., H Hu, M. Garshasbi, et al., "Deep sequencing reveals 50 novel genes for recessive cognitive disorders", *Nature*, Vol. 478, No. 7367, 2011, pp. 57-63.

Prainsack, Barbara, Jenny Reardon, Richard Hindmarsh, et al., "Personal genomes: Misdirected precaution", *Nature*, Vol. 456, No. 2008, pp. 34-35.

Prainsack, Barbara, and R. Hindmarsh, "Beyond borders: trends and challenges in global forensic profiling and databasing", in Barbara Prainsack and R. Hindmarsh (eds.), *Genetic Suspects: Global Governance of Forensic DNA Profiling and Databasing*, Cambridge University Press, Cambridge, 2010, pp. 333-341.

Pray, Leslie, "DTC Genetic Testing: 23andme, DNA Direct and Genelex", *Nature Education*, Vol. 1, No. 1, 2008, pp. http://www.nature.com/scitable/topicpage/DTC-Genetic-Testing-23andme-DNA-Direct-and-674.

Ropers, Hans Hilger, "Genetics of Early Onset Cognitive Impairment", *Annual Review of Genomics and Human Genetics*, Vol. 11, No. 2010, pp. 161-187.

Sanger, F., S. Nicklen and A.R. Coulson, "DNA sequencing with chain-terminating inhibitors", *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 74, No. 12, 1977, pp. 5463-5467.

Stajano, Frank, Lucia Bianchi, Pietro Liò,and Douwe Korff, "Forensic genomics: kin privacy, driftnets and other open questions", in Vijay Atluri and Marianne Winslett (eds.), *Proceedings of the 2008 ACM Workshop on Privacy in the Electronic Society*, WPES 2008, Alexandria, VA, USA, October 27, 2008, ACM, New York, 2008, pp. 15-22.

Staley, Kristina, "The police National DNA Database: balancing crime detection,human rights and privacy", GeneWatch UK, Buxton 2011.

Tavani, H. T., "Genomic research and data-mining technology: implications for personal privacy and informed consent", *Ethics and information technology*, Vol. 6, No. 1, 2004, pp. 15-28.

The International Human Genome Sequencing Consortium, "Finishing the euchromatic sequence of the human genome", *Nature*, Vol. 431, No. 7011, 2004, pp. 931-945.

Van Camp, N., and K. Dierickx, "The retention of forensic DNA samples: a socio-ethical evaluation of current practices in the EU", *Journal of Medical Ethics*, Vol. 34, No. 8, 2008, pp. 606-610.

Venter, J. Craig, Mark D. Adams, Eugene W. Myers, et al., "The sequence of the human genome", *Science*, Vol. 291, No. 5507, 2001, pp. 1304-1351.

Weale, Albert, Hugh Perry, et al., "Medical profiling and online medicine: the ethics of 'personalised healthcare' in a consumer age", Nuffield Council on Bioethics, London, 2010.

Wjst, Matthias, "Caught you: threats to confidentiality due to the public release of large-scale genetic data sets", *BMC Medical Ethics*, Vol. 11, No. 1, 2010, pp. 21.

Zhang, J., R. Chiodini, A. Badr and G. Zhang, "The impact of next-generation sequencing on genomics", *Journal of Genetics and Genomics*, Vol. 38, No. 3, 2011, pp. 95-109.

Chapter 7, Technologies for Human Enhancement and their impact on privacy

Philip Schütz and Michael Friedewald,
Fraunhofer ISI

7.1 INTRODUCTION

The secret of the evolutionary success of the human species is their insatiable hunger for learning and improvement. Reflected in a multitude of tales, fables and comics, the notion of a *homo superior*, who stands out from the crowd due to his/her extraordinary mental or physical abilities, runs like a golden thread not only through world literature but also through science, politics and philosophy.

Excluding the highly dynamic field of genetic enhancement as a separate case (see also case study on whole DNA sequencing), the origins of human enhancement mainly developed in the technical and pharmacological science and research arena. Since humans started to use tools in order to increase their chances of survival, technical approaches were always at the forefront of enhancing human performance. However, the ancient Greek myth of *Icarus and Daedalus*, who succeed in flying with the help of hand-crafted wings, but later suffered from Icarus' arrogance and the fallibility of their own invention, allegorises the dilemma that the development of ground-breaking technologies is frequently accompanied by fatal consequences.

This is also true regarding pharmaceutical enhancement and the example of invention of today's famous illegal drug *heroin*, which was named after the supposed heroic effects on users by the German company Bayer in 1895. Though originally designed to protect users against various illnesses and maladies, the artificial drug turned out to be one of the most addictive and dangerous pharmaceutical substances ever created. Another form of enhancement is the practice of doping. Whereas the attempt to increase physical performance through synthetic illegal substances is socially condemned, especially in sports, ground-breaking progress in brain research, the massive expansion of nanotechnology and the phenomenon of "converging technologies" has opened up new opportunities for human enhancement on another level.

It is noteworthy that the starting point of this case study is the concept of human enhancement rather than a concrete technology with enhancement features. An essential part of this paper is devoted to a discussion of the term "human enhancement", which is, in fact, marked by huge definitional and conceptual problems, before discussing practical examples of applications with potential relevance to aspects of privacy and data protection. However, some of these human enhancement applications are characterised by their early stage of development and their potential relevance in the mid- to long-term future, and in most cases are still far away from being introduced to the mass market.

Whereas data protection in the context of human enhancement is only touched upon when technologies with the capability of collecting and processing personal data are involved, privacy is almost always relevant when the enhancement implies the implantation of a technology into the human body or the taking of pharmaceutical substances to influence human behaviour. The feature of transcending boundaries is central to human enhancement, posing new questions and challenges to privacy and data protection. [882]

[882] Cuhls, Kerstin, Walter Ganz, Philine Warnke, et al., *Foresight-Prozess im Auftrag des BMBF: Zukunftsfelder neuen Zuschnitts*, Fraunhofer ISI, Fraunhofer IAO, Karlsruhe/Stuttgart, 2009; Beckert, Bernd, Bruno Gransche, and Philine Warnke, *Mensch-Technik-Grenzverschiebung - Perspektiven für ein neues Forschungsfeld*, Fraunhofer Verlag, Stuttgart, 2011.

7.2 HUMAN ENHANCEMENT – AN OVERVIEW

The term "human enhancement" is highly controversial because the idea not only conveys an ideological conflict, but also remains imprecise about how the enhancement should take place. Serving as a starting point, the working definition of this paper focuses on the assumption that human enhancement is about "*boosting our capabilities beyond the species-typical level or statistically-normal range of functioning for an individual*".[883]

7.2.1 Attempts to categorise "Human Enhancement"

The idea of improving ourselves in order to better survive seems to be inherent to human nature. The process of improvement comprises the goal of conditioning and adapting the human body to the challenges of the environment basically in terms of *mental* and *physical training*. The development and usage of tools has been a decisive feature of human evolution because it not only increased the chances of survival but also functioned as a catalyst to boost learning processes and especially mental abilities.[884]

Here, the often proposed **distinction** between **"*natural*"** and **"*artificial*" enhancement** comes into play. Whereas the first refers to the improvement of our minds and bodies through e.g. education, communication, reasoning, meditation, diets and physical exercises, the latter points to the deployment of tools and technologies. The problem with this distinction is that both attributes are vague and, in fact, interrelated. When it comes to education, for example, reading a book would definitely be considered a "natural" means of cognitive enhancement. However, a book could be regarded as a tool that fosters intellectual learning processes, which suggests that the natural-artificial distinction does not imply the actual meaning of these attributes but rather the individual perception linked to it. "Natural" could therefore be described as "normal" and "socially accepted", while the attribute "artificial" comprises notions of strangeness and unfamiliarity. Thus, the debate about human enhancement is highly subjective and context-dependent, often charged with emotions. Nevertheless, these perceptions are decisive when it comes to the acceptance and successful adaptation and implementation processes, or the rejection of enhancement products.

Another attempt to distinguish human enhancement comprises its **separation from medical therapy**. That way, high-tech prostheses, for instance, would not be considered an enhancement technology as long as they are not boosting patients' physical performances to a significantly higher level than to be expected of an average person. Following this line of argument, the carbon-fibre prosthetics of the South African sprinter Oscar Pistorius, who was born with a congenital disorder in his legs (which were afterwards amputated halfway between his knees and ankles[885]), would not represent an enhancement technology in the classical sense,

---

[883] Allhoff, Fritz, Patrick Lin, James Moor and John Weckert, *Ethics of Human Enhancement: 25 Questions & Answers*, Report prepared for the US National Science Foundation under awards # 0620694 and 0621021, Human Enhancement Ethics Group, 2009, p. 8. http://www.humanenhance.com/
For two influential agenda setting documents see Roco, Mihail C., and William Sims Bainbridge (eds.), *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science*, Kluwer, Dordrecht, 2003 and Nordmann, Alfred, "Converging Technologies - Shaping the Future of European Societies", EUR 21357, Office for Official Publications of the European Communities, Luxembourg, 2004.

[884] See for instance Gehlen, Arnold, *Die Seele im technischen Zeitalter. Und andere soziologische Schriften und Kulturanalysen [1957]*, Vittorio Klostermann, Frankfurt, 2004.

[885] Longman, Jeré, "An Amputee Sprinter: Is He Disabled or Too-Abled?", *New York Times*, 15 May 2007, http://www.nytimes.com/2007/05/15/sports/othersports/15runner.html?_r=1&oref=slogin

since they are meant to provide leg-amputees with the ability to walk or run on a level comparable to that of any healthy individual or athlete.

Nonetheless, the International Association of Athletics Federations (IAAF), which did not allow Pistorius to participate in normal competitions, including the Olympic Games, argued that his prosthetics would give him an unfair advantage over other athletes.[886] Although the Court of Arbitration for Sport (CAS) reversed this decision a few months later,[887] the debate remains controversial, taking into account that future prosthesis will literally outrun natural limbs in respect to their performance, efficiency, resilience and other aspects.

Thus, the therapy-enhancement distinction can not only be contested in regards to the targeted level of performance, but also because the lines between medical and non-medical purposes are blurred. Technologies such as the mental typewriter or brain-to-robot applications,[888] which were often originally designed for therapeutic purposes in order to help (fully) paralysed persons to better manage their lives, could be used for enhancement purposes as well.

Finally, the term "medical therapy" turns out to be in itself imprecise, at least when it comes to preventive medical approaches. Vaccinations, for example would certainly reduce specific infection risks. Therefore, they could also be seen as an enhancement factor. Yet, their quasi-medical purpose of immunisation also suggests a certain form of preventive therapy. Thus, the question arises: Could a technology that has preventive characteristics in terms of the health status of an individual be considered as human enhancement?

In order to discriminate between human enhancement and the mere use of tools, the **internal-external distinction** is often used in relevant literature. Normally, human enhancement is supposed to have effects within the human body, which is clearly the case when considering pharmaceutical and genetic enhancement. But the majority of technologies with human enhancement potential, such as brain computer interfaces (BCI) or virtual retina displays, were developed to operate outside the human body. Supported by the trend of technological miniaturisation and the growing importance of nanotechnology, a number of scholars assume that these technologies will be implanted into human bodies in the near future.[889] However, ICT implants, especially those with human enhancement features are still an exception.

Summing up, these three distinctions patterns, which can be found in several comprehensive reports and studies,[890] represent an approximation of what is actually meant by human en-

---

[886] Knight, Tom, "IAAF call time on Oscar Pistorius' dream", *Telegraph*, 10 Jan 2008, http://www.telegraph.co.uk/sport/othersports/athletics/2288489/IAAF-call-time-on-Oscar-Pistorius-dream.html

[887] Dunbar, Graham, "Double-amputee wins appeal to aim for Olympics", *The Independent*, 16 May 2008. http://www.independent.co.uk/sport/general/athletics/doubleamputee-wins-appeal-to-aim-for-olympics-829647.html

[888] Both applications are based on brain computer interface (BCI) technologies, which will be discussed in the following.

[889] Theißen, Sascha, *Risiken informations- und kommunikationstechnischer (IKT-) Implantate im Hinblick auf Datenschutz und Datensicherheit*, Universitätsverlag Karlsruhe, Karlsruhe, 2009; Coenen, Christopher, Stefan Gammel, Reinhard Heil, and Andreas Woyke (eds.), *Die Debatte über "Human Enhancement": Historische, philosophische und ethische Aspekte der technologischen Verbesserung des Menschen*, Transcript Verlag, Bielefeld, 2010.

[890] Cf.: U.S. President's Council on Bioethics, "Beyond Therapy - Biotechnology and the Pursuit of Happiness", 2003; Allhoff, et al., op. cit., 2009; Science and Technology Options Assessment (STOA), "Human Enhancement Study", European Parliament, 2009; Eckhardt, Anne, Andreas Bachmann, Michèle Marti et al.,

hancement (cf. Figure 1). Today, virtually no technology fulfils every feature as seen in Figure 3. Instead, the technologies and pharmaceutical substances that will be analysed in this case study possess **single** enhancement characteristics. Furthermore, the selection of technologies not only considers aspects of human enhancement, but also the potential for privacy infringements central to the PRESCIENT project. Since privacy and data protection issues are particularly affected and highly relevant in the medical field, the therapy-enhancement distinction will probably be the one which has the least relevance for our purposes. That is why some of the discussed technologies in the following may appear to belong to the medical application area. However, they should be regarded in terms of their enhancement features and opportunities of prospective enhancement usages.

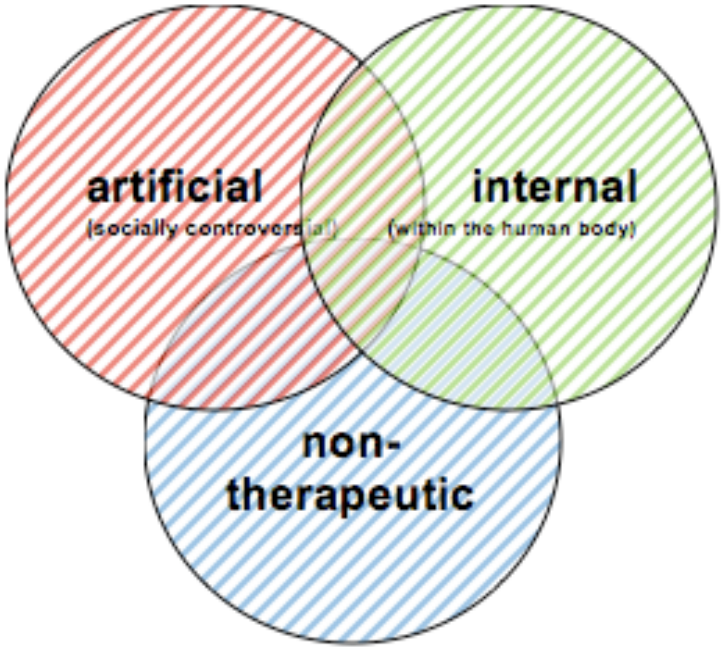


Figure 7.1: Central features of Human Enhancement

7.2.2 Various fields of applications

Distinctions of technologies

As mentioned, human enhancement can be roughly divided into three fields of applications: pharmacological, technical and genetic enhancement.[891] Since DNA-sequencing is already

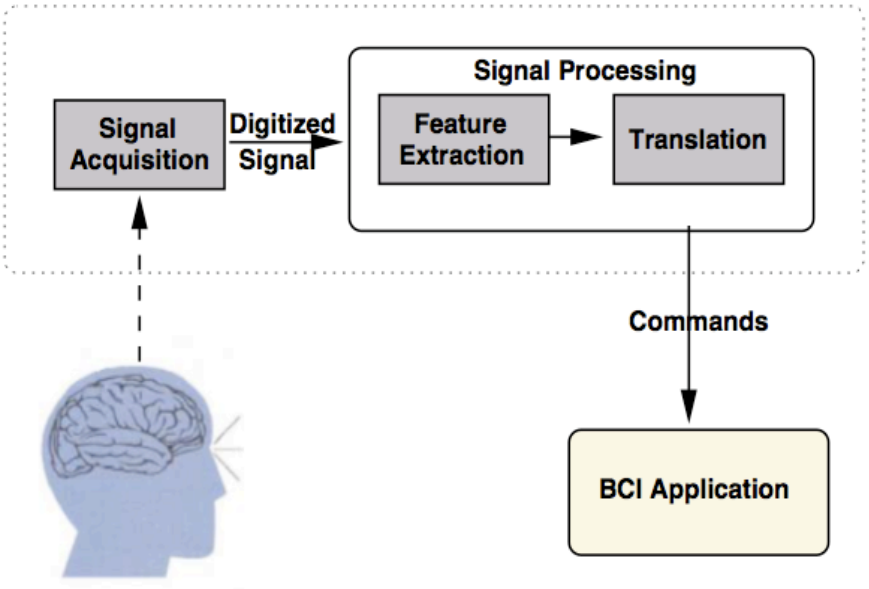
Human Enhancement, vdf Hochschulverlag, Zürich, 2011; Science and Technology Options Assessment (STOA), "Making Perfect Life: Bio-engineering (in) the 21st Century", European Parliament, 2011.

[891] Reschke, Stefan, "Verbesserung menschlicher Leistungsfähigkeit", in Fraunhofer INT (ed.), *Jahresbericht 2009*, Fraunhofer-Institut für naturwissenschaftlich-technische Trendanalysen, Euskirchen, 2010, pp. 18-19; Andler, Daniel, Simon Barthelmé, Bernd Beckert, et al., *Converging technologies and their impact on the social sciences and humanities (CONTECS): An Analysis of critical issues and a suggestion for a future research agenda*, Final Report, 2008. http://www.contecs.fraunhofer.de/; Beckert, Bernd, Clemens Blümel, and Michael

dealt with in another case study, the following sections will focus on the first two fields of applications. Hence, one technical and one pharmacological example will be examined in more detail now.

Brain Computer Interfaces (BCIs)

The Brain-Computer Interface Project (cf. Figure 2), which was launched in the early 1970s at the University of California by a team of researchers led by Jacques Vidal, marked a new starting point in the field of biocybernetics and human computer interaction. The project was based on the conviction that electroencephalography (EEG) waves "contain usable concomitances of conscious and unconscious experiences and that the set of continuous electric signals observed does not for the most part consist of random noise as was often suggested, but on the contrary, constitutes a highly complex but significant mixture that reflects underlying neural events."[892] Alongside magnetoencephalography (MEG), functional magnetic resonance imaging (fMRI) and near-infrared systems (fNIR), EEG is probably the most prevalent neuroimaging technique due to its low cost, small size and ease of use as well as the fact that "electrophysiological features represent the most practical signals for BCI applications today."[893]



Source: (Thorpe et al. 2005).

Figure 7.2: Basic design of a BCI system

Since the brain consists of billions of neurons, which process and transmit information by electrical and chemical signalling, brain activity creates electrical impulses that can be meas-

---

Friedewald, "Visions and Realities in Converging Technologies: Exploring the technology base for convergence", *Innovation - The European Journal of Social Science Research*, Vol. 20, No. 4, 2007, pp. 375-394.

892 Vidal, Jacques J., "Toward direct brain-computer communication", *Annual review of Biophysics and Bioengineering*, Vol. 2, No. 1, 1973, pp. 157–180 [p. 164].

893 McFarland, Dennis J., and Jonathan R. Wolpaw, "Brain-computer interfaces for communication and control", *Communications of the ACM*, Vol. 54, No. 5, 2011, pp. 60-66 [p. 63]. For an overview of neuroimaging technologies see Hüsing, Bärbel, Lutz Jäncke and Brigitte Tag, *Impact Assessment of Neuroimaging*, IOS Press, Amsterdam, 2006.

ured. On the one hand, non-invasive forms of EEG technology draw on electrodes that are placed on the scalp in order to detect these electrical impulses. Although the temporal resolution of EEG to measuring changes in neuronal activity is very good, non-invasive forms are prone to rather poor spatial resolution, i.e. determining the precise position of active sources in the brain, as well as artefacts arising from muscle and eye movements.[894]

Invasive ways of installing EEG technology, e.g. by implanting electrodes within the skull directly onto the cortex, provide, on the other hand, a much more precise and effective measurement of electrical impulses, which, however, "requires surgery and [therefore] carries the risk of infection or brain damage."[895] Thus, invasive methods are rarely used, except for urgent medical purposes such as locating and monitoring epilepsy. Another often-neglected aspect of invasive EEG technology, which will be discussed more thoroughly in one of the following sections, is its impact on the carrier's personality and self-perception, including the fear of external control.[896]

Whereas EEG, as the most common technology involved in BCIs, only comprises the technique to measure brain activity, BCI technology as a whole involves a much wider range of complex software and hardware that is supposed to translate the neuronal signals into commands that operate eventually a device.[897] Since EEG technology, as pointed out above, does not locate the origin of the electrical impulses perfectly precisely, approximate values have to be constructed in order to link specific actions to particular neuronal signals. Most importantly, this allocation process is continuously improved by learning and adjusting on both sides: human and computer. Gerven et al. have called this adaption process between user and the computer, the *BCI cycle.* The cycle is repeated in a loop to improve the desired outcome. Key stages are: Measurement, pre-processing, extraction of relevant features, prediction of an outcome (supposed to reflect the user's intention), output and finally, execution of a task as well as a repeated often visual stimulation of the user so that he/she can adjust his/her mental activity to the output of the computer.[898]

Furthermore, users are not only obliged to learn to control the neuronal firing rate, i.e. the intensity of brain activity, in order to move, for example, a cursor on a screen,[899] they also

---

[894] van Gerven, Marcel, Jason Farquhar, Rebecca Schaefer et al., "The brain–computer interface cycle", *Journal of Neural Engineering*, Vol. 6, No. 4, 2009, pp. 1-10 [p. 2].

[895] Ortiz Jr., Sixto, "Brain-Computer Interfaces: Where Human and Machine Meet", *IEEE Computer*, Vol. 40, No. 1, 2007, pp. 17-21 [p. 17].

[896] Another distinguishing feature of BCI technology is their direction of operation, Consequently, BCIs mirror data about brain activity onto a computer. So-called computer brain interfaces (CBIs) work the other way around, sending out electrical signals to the brain. They are capable of infringing upon the carrier's privacy on a totally new level.

For example, drawing on the implantation of impulse-giving electrodes into the malfunctioning region of the brain, deep brain stimulation (DBS) offers a treatment option for Parkinson's, which is characterised by a dysfunction of a pea-sized part of the brain, the so-called *Nucleus subthalamicus* (cf. Raabe, Kristin, "Stimulieren ohne Nebenwirkungen", *Technology Review (Deutsche Ausgabe)*, Vol. 8, 2011, pp. 10-11). Since this nucleus is right next to the limbic system, which is widely considered to be responsible for various personal traits, it is not surprising that attempts to penetrate this region can result in a serious personality change of the patient.

Although CBIs, and particularly DBS, mostly comprise medical forms of applications these days, future enhancement usages could be possible in cases such as implantable neuro-memory chips (cf. Maguire, G. Q., and Ellen M. McGee, "Implantable Brain Chips? Time for Debate", *The Hastings Center Report*, Vol. 29, No. 1, 1999, pp. 7-13. http://www.jstor.org/stable/3528533).

[897] McFarland and Wolpaw, op. cit., 2011, p. 62.

[898] van Gerven, et al., op. cit., 2009, p. 2.

[899] McFarland and Wolpaw, op. cit., 2011, p. 62.

have to be able to activate specific neuronal impulses e.g. by concentrating (only mentally) on a continuous movement of the left hand. The computer, on the other hand, has to identify the user's intention step by step. All of this requires a time-consuming learning process in which the user has to be trained in order to achieve a precise transfer of his thoughts to the machine.[900]

Normally, BCIs are used for the purpose of communicating or physically controlling an object. Although this does not necessarily imply activities that lie beyond the "species-typical level or statistically-normal range of functioning for an individual", the method of transferring commands to a machine without depending on neuromuscular control introduces a variety of new and ground-breaking enhancement opportunities. BCI technology allows people to physically interact with the world around them without muscle control, i.e. first and foremost without using their hands or moving their lips. Here, the aforementioned lines between medical and non-therapeutic applications become blurred. Often originally designed for therapeutic purposes in order to help (fully) paralysed people to better manage their lives, BCI technology could be deployed for human enhancement as well.

BCIs which allow amputees to mentally control high-tech prosthesis[901] can already be seen as an enhancement technology if, for instance, the power of an artificial hand surpasses that of a normal one, making it possible for the user to e.g. crush stones. Another form of supporting, and/or enhancing, physical movements would be the idea of a mentally-controlled exoskeleton, being currently developed by an EU-funded project, named *mind walker*, which primarily aims at conceiving of a system that empowers people with lower limb paralysis to walk again and perform usual daily activities in the most autonomous and natural manner.[902]

A further example of BCI applications that is mentioned regularly in the press and in scientific literature is the so-called *mental typewriter*.[903] This device provides the trained user with the ability to communicate through a computer screen, typewriting the desired questions, commands or statements without the movement of any part of his/her body. Although the mental typewriter has to be calibrated to the individual brain wave pattern of the user, researchers in the Berlin BCI (BBCI) project have succeeded in developing an interface that facilitates and accelerates the otherwise complex and laborious learning process on both sides.[904] This could revolutionise methods of physical control and communication for severely handicapped, immobile patients, such as people with, for example, locked-in syndrome, who are only able to move their eyes, while being totally awake and aware of things happening around them.

---

[900] The EU-funded project BRAIN (Bcis with Rapid Automated Interfaces for Non-experts) aims to speed up and facilitate this often complicated learning process so that especially users with severe physical impairments can more easily take advantage of BCI technologies. Cf.: http://www.fastuk.org/research/projview.php?id=1449

[901] Yahud, Shuhaida, and Noor Azuan Abu Osman, "Prosthetic Hand for the Brain-computer Interface System", in Ibrahim, Fatimah, Noor Azuan Abu Osman et al. (eds.), *3rd Kuala Lumpur International Conference on Biomedical Engineering 2006*, Springer, Berlin, Heidelberg, 2007, pp. 643-646. http://www.springerlink.com/index/10.1007/978-3-540-68017-8_162

[902] https://mindwalker-project.eu/

[903] Krepki, Roman, Gabriel Curio, Benjamin Blankertz and Klaus-Robert Müller, "Berlin Brain–Computer Interface—The HCI communication channel for discovery", *International Journal of Human-Computer Studies*, Vol. 65, No. 5, 2007, pp. 460-477.

[904] Next to the BBCI project, the Fraunhofer Institute for Computer Architecture and Software Technology FIRST also participated in the research of BCI applications that were aimed at giving control over the movements of robots; cf.: The Brain2Robot Project; http://www.first.fraunhofer.de/projekte/brain2robot/

Finally, the short period of training, as well as the simplification of the setup, are essential requirements for BCI applications in computer games. The EEG cap, for example, should not be characterised by lengthy electrode positioning or the need for conductive gel or time-consuming clean-up after a session. Instead, so-called dry caps are being developed.[905] According to Nijholt, there are two main areas relevant for the development of BCIs in games and entertainment:

1. "to collect information from brain activity that informs us about the cognitive state of the user [...]
2. to develop applications where information derived from brain activity allows us to control an application."[906]

The first is particularly interesting in the context of *affective computing*, i.e. adjusting computer processes to the emotional state of the user. That way a customised adaption of a game or an interface to the user is possible, for instance, in order to raise or decrease the difficulty of a task in a game. The second application area provides the gamer with novel and unique game control opportunities. Due to the highly competitive market, the gaming and entertainment industry welcomes innovation and, at first, even seemingly unusual technologies such as the motion capture technology which successfully entered the mass market with Nintendo's gaming platform *Wii* in 2006.

Neuro-enhancing pharmaceuticals (neuro-enhancers)

Contrary to doping in sports, this section deals with pharmaceutical enhancement on a cognitive and emotional level. Since the 1990s, psychoactive substances have been increasingly used illegally, in order to meet the requirements of today's meritocracy (a performance-based society).[907] Although the enhancing effects of pharmaceuticals on cognitive and emotional capabilities are highly contested, and can have serious adverse reactions,[908] the idea of boosting cognitive skills beyond the average, including the ability to focus, remains attractive, especially for individuals who are under pressure to perform and succeed in societies based on knowledge and the appreciation of the same.

Characterised by its biological and chemical effects, pharmaceutical neuro-enhancement comprises not only illegal drugs such as amphetamine or cocaine, but also legal medical products, i.e. either available on prescription (off-label use is possible), e.g. antidepressants and methylphenidate (Ritalin), or OTC (over-the-counter) drugs such as Aspirin.[909]

---

[905] Fraunhofer FIRST research project "Speed Cap – Gelfreies EEG", 2011. http://www.first.fraunhofer.de/projekte/speed_cap_gelfreies_eeg/

[906] Nijholt, Anton, "BCI for Games: A 'State of the Art' Survey", in Stevens, Scott M., and Shirley J. Saldamarco (eds.), *Entertainment Computing - ICEC 2008*, Springer, Berlin, Heidelberg, 2009, pp. 225-228 [p. 225]. http://www.springerlink.com/index/10.1007/978-3-540-89222-9_29

[907] Eckhardt, et al., op. cit., 2011, p. 9.

[908] Repantis, Dimitris, "Die Wirkung von Psychopharmaka bei Gesunden", in Wienke, Albrecht, Wolfram Eberbach et al. (eds.), *Die Verbesserung des Menschen*, Springer, Berlin, Heidelberg, 2009, pp. 63-68. http://www.springerlink.com/index/10.1007/978-3-642-00883-2_5

[909] Often justified with the argument of helping people with dementia, molecular memory boosters such as insulin growth factor II (IGF-II) represent another example of neuro-enhancement, drawing on manipulation of cerebrovascular functions, i.e. increasing the blood supply/flow within the brain; cf.: Gräff, Johannes, and Li-Huei Tsai, "Cognitive enhancement: A molecular memory booster", *Nature*, Vol. 469, 2011, pp. 474-475. http://www.nature.com/doifinder/10.1038/469474a

However, the potential impact on privacy and data protection is crucial to this case study. Whereas the latter can easily be neglected, the first comprises a highly relevant dimension in the context of neuro-enhancers due to the fact that privacy is not only linked to the notion of self-determination, but can also be seen as a shield against external control over oneself (heteronomy). Even though the concept of human enhancement implies a certain degree of voluntary and self-determined action by the user, the prescribed usage of neuro-enhancers such as Ritalin raises privacy issues due to the involvement of a third party, e.g. medics, teachers, parents, etc., that attempts to exercise control over the recipient. As one of the most famous examples, Ritalin is supposed to medicate people with a so-called attention deficit hyperactivity disorder (ADHD). It is assumed that the drug increases the alertness and concentration of its users by blocking certain senses.

However, diagnosis of ADHD and the effectiveness of Ritalin as medication are highly contested by the scientific community. Farah, for instance, points to the fact that there is a "widespread use of psychopharmacology by people who would not have been considered ill twenty years ago."[910] Nonetheless, Ritalin has prevailed becoming increasingly prevalent on the mass market with continuous growth in user numbers, particularly in the US, but also in Europe.[911] Especially off-label usage is estimated as very high: Ritalin is not only used by high school and college students in order to enhance their ability to focus before and during exams, but even wide spread among elementary school children, who often feel pressured to improve their performance in school.[912] Whether or not Ritalin is subject to off-label usage, a staff background paper from the US-President's Council on Bioethics comes to the conclusion that "the diagnosis of ADHD and prescription of stimulants to treat it are currently affecting millions of American schoolchildren. [...] Groups of children visit the school nurse for their Ritalin as part of their daily routine. Others take the only dose they need in the morning. Ritalin has thus entered the practice of schooling and the culture into which our youngest citizens are inducted."[913]

Furthermore, modafinil, which increases the ability to stay awake and focused, represents a more and more popular and prevalent neuro-enhancer. The drug is often subject to off-label usage not only by the military, police forces and astronauts, but also students and mostly young professionals who face a lot of stress and long working hours; cf.: Frean, Alexandra, and Patrick Foster, "Cheating students turn to smart drug for edge in exams", *The Sunday Times*, 23 Jun 2007. http://www.timesonline.co.uk/tol/news/uk/education/article1975271.ece
A comprehensive study of the German public health insurance fund DAK comes to the conclusion that 24 per cent of consumers of modafinil in Germany lack a proper medical explanation for their consumption of modafinil. cf.: DAK, "Gesundheitreport 2009. Analyse der Arbeitsunfähigkeitsdaten. Schwerpunktthema Doping am Arbeitsplatz. Deutsche Angestellten Krankenversicherung", Deutsche Angestellten Krankenversicherung, 2009, p. 69. http://www.dak.de/content/filesopen/Gesundheitsreport_2009.pdf

[910] Farah, Martha J., "Neuroethics: The practical and the philosophical", *Trends in Cognitive Sciences*, Vol. 9, No. 1, 2005, pp. 34-40 [p. 35].

[911] In 2009, the products Ritalin and Focalin, both used as medication against ADHD, achieved annual sales of 449 million US dollars worldwide, 343 million US dollars on the US-market; cf. Novartis, *Novartis erzielt 2009 Rekordergebnisse - Neu eingeführte Produkte erweisen sich als Wachstumstreiber*, Financial Report, Basel, 2010. http://hugin.info/134323/R/1377020/338142.pdf

[912] See Kapner, Daniel Ari, "Recreational use of Ritalin on College Campuses", Higher Education Center, 2008. http://www.higheredcenter.org/services/publications/recreational-use-ritalin-college-campuses

[913] Council on Bioethics, *Human flourishing, performance enhancement, and Ritalin*. Staff background paper. The President's Council on Bioethics, 2002.
http://bioethics.georgetown.edu/pcbe/background/humanflourish.html

Figure 3 maps pharmaceutical neuro-enhancers, BCI and other exemplary technologies in regards to the three central features of human enhancement. The technologies depicted are moreover distinguished in terms of their state of development.

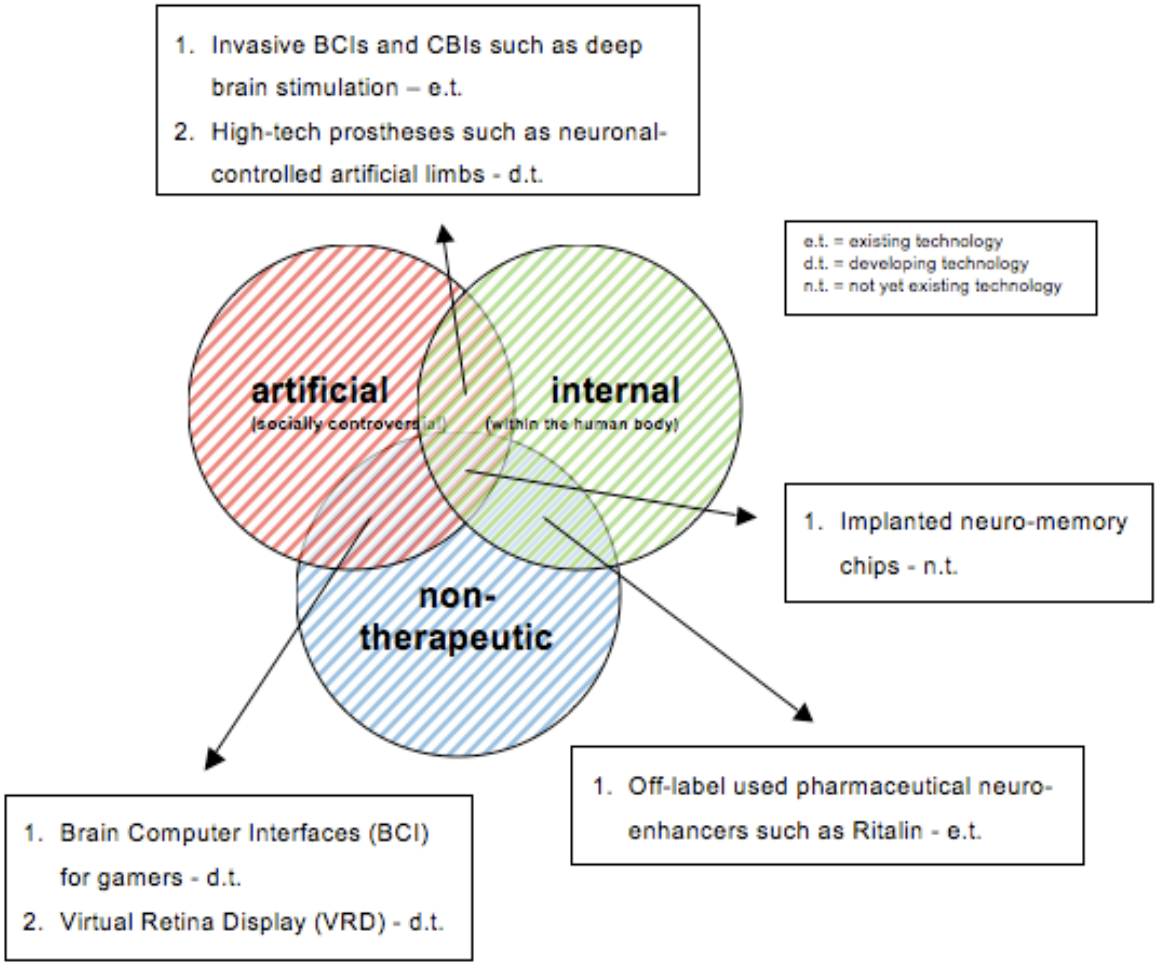


Figure 7.3: Technologies allocated to human enhancement features

7.2.3 Actors and beneficiaries of human enhancement

The following section will briefly outline the most important actors who are shaping the present state of discussed technologies (BCIs and neuro-enhancers) and could decisively influence their future development

(Public) health sector

The public health sector in many OECD countries is currently undergoing significant change. Preventive medicine and personal responsibility (especially healthy living) is becoming more and more important, not only due to the immense increase in costs of therapies. This development fosters a self-reliant behaviour on the part of the individual, providing incentives to pursue more proactive and healthy lifestyles also based on the idea of better and longer-lasting mental as well as physical performance. Thus, former patients become self-determining consumers of biomedical services, changing the traditional doctor-patient relationship. Medical treatment no longer serves the primary purpose of healing, but is rather di-

rected towards the satisfaction of the customer, exemplified by the continuous growth of plastic surgeries, also a particular form of human enhancement.[914]

Yet, human enhancement may contain unknown risks to the (long-term) health of the recipient. That is why there is a broad spectrum of adversaries questioning technological developments in general. Nonetheless, a more and more technologised and performance-orientated society seems to be the dominant trend, paving the way for a culture of physical and mental enhancement. Since the medical applications of BCIs are in their infancy, their practicability in the public health sector as well as acceptance in society, both representing key requirements for bringing them on the market, must still be proven. For individual cases such as that of patients with locked-in syndrome, BCIs certainly provide a unique opportunity to regain control of and communication with their environment.

In contrast, the usage of neuro-enhancing pharmaceuticals is much more prevalent in OECD countries, which makes the impact of neuro-enhancers on societies a highly relevant subject. The public health sector seems to rely more and more on drugs in order to combat supposedly severe mental illnesses such as ADHD, which also results in off-label usages to counter poor concentration or tiredness of otherwise healthy individuals.

Law enforcement and military actors

Even though BCI technology is at the very beginning of its development, the data gained from measuring brain activity, i.e. the unique electrical impulses and wave patterns of individuals, comprise, at least potentially, valuable and highly sensitive information. Indeed, law enforcement authorities could be interested in such data, which can be used not only to unambiguously identify an individual, but also to find out about certain dispositions that make the data subject more or less prone to commit a crime.[915] Moreover, there are various ways of deploying BCI technology for investigative purposes such as lie detection or guilty knowledge tests.[916]

Despite these applications and the high-quality of potential surveillance data, BCIs could be further developed in two directions, i.e. from human to machine and vice versa. While the notion of a functioning digital input directly into the human brain is still a futuristic scenario, the impact of such a technology on personal privacy and the concept of self-control would be devastating. However, the military or intelligence services could conceivably also be interested in such technologies, for example in their potential to remotely control double agents or enemy combatants.

As already mentioned, neuro-enhancing pharmaceuticals such as modafinil, i.e. a drug that increases the ability to stay awake and focused, are quite frequently used by police and military forces when special situations require high concentration and long-lasting alertness.[917] Additionally, neuro-enhancers, in the context of "therapeutic forgetting", could be of interest

[914] Eckhardt, et al., op. cit., 2011, p. 133.
[915] Kepecs, Adam, "Neuroscience: My brain made me do it", *Nature*, Vol. 473, 2011, pp. 280-281. http://www.nature.com/doifinder/10.1038/473280a
[916] Al-Sagban, Mariam, Omnia El-Halawani, Tasneem Lulu, et al., "Brain computer interface as a forensic tool", in *5th International Symposium on Mechatronics and Its Applications*, IEEE, Amman, 27-29 May 2008, pp. 1-5.
[917] Baranski, Joseph V., Ross Pigeau, Peter Dinich and Ira Jacobs, "Effects of modafinil on cognitive and metacognitive performance", *Human Psychopharmacology: Clinical and Experimental*, Vol. 19, No. 2004, pp. 323-332. http://doi.wiley.com/10.1002/hup.596

for the military, as returning soldiers are often affected by traumatic memories of experiences in war.[918]

Industry

Because BCI technology has not yet entered the mass market successfully, no dominant manufacturing or engineering company of either BCI hardware or software has emerged. That is why current BCI technologies and applications are a niche product, mostly developed by small and medium-sized enterprises (SMEs) or research institutes.

The collection, storage and processing of highly sensitive data gained from individuals using BCIs could comprise a new segment in the flourishing market for personal data. Drawing on neuroscience, particularly neuromarketing, which is meant to locate consumers' "buy buttons", in order to get closer to opening the "black box" of the consumer's mind,[919] would open up promising opportunities to exploit the collected data of BCI users. It has always been a marketing dream of any company to advertise their products, services or information in a way that a potential buyer is unable to resist. Neurmarketing offers realistically a chance to reach this goal.

As opposed to the BCI business, the pharmaceutical industry is already one of the largest and most influential branches in the private sector. Due to decreasing innovation efficiency and increasing price regulation in Europe, pharmaceutical companies are confronted with challenging times.[920] Thus, the tapping of new markets is crucial. Performance-enhancing drugs represent such a new market into which some medical products like Ritalin have already successfully entered.

Academia

The academic and scientific community seems to be of vital importance, not only when it comes to the development of human enhancement technologies, but also in having influence on societal acceptance or rejection of these technologies. Woyke distinguishes four ideal-typical positions, which underlie the set of moral and ethical values of researchers working in the field of human enhancement: [921]

1. The *transhumanist* argues in favour of the legitimacy and even necessity of human enhancement, since self-transcendence, i.e. the desire to improve and better ourselves, and therefore the crossing of ethical, moral and cultural borders is an inherent part in the nature of humans. [922]

---

[918] Evers, Kathinka, "Perspectives on Memory Manipulation: Using Beta-Blockers to Cure Post-Traumatic Stress Disorder", *Cambridge Quarterly of Healthcare Ethics*, Vol. 16, No. 2, 2007, pp. 138-146 [p. 144]. http://www.journals.cambridge.org/abstract_S0963180107070168 ibid

[919] Editorial, "Brain scam?", *Nature Neuroscience*, Vol. 7, No. 7, 2004, pp. 683, Moore, Karl, "Maybe it is like brain surgery: How neuromarketing is using brain scan technologies to give new insights into the "black box" of the consumer mind", *Marketing Magazine*, Vol. 110, No. 14, 2005, pp. 12.

[920] Eckhardt, et al., op. cit., 2011, p. 138.

[921] Woyke, Andreas, "Human Enhancement und seine Bewertung – Eine kleine Skizze", in Coenen, Christopher, Stefan Gammel et al. (eds.), *Die Debatte über "Human Enhancement": Historische, philosophische und ethische Aspekte der technologischen Verbesserung des Menschen*, Transcript Verlag, Bielefeld, 2010, pp. 21-40. [p. 24]

[922] Coenen, Christopher, "Utopian Aspects of the Debate on Converging Technologies", in Gerhard Banse and Imre Hronszky, et al. (eds.), *Converging Technologies. Promises and Challenges*, Sigma, Berlin, 2007, pp. 141-172.

2. Emphasising the changeability of the idea of human nature, *liberal ethicists* support a sophisticated evaluation of human enhancement technologies, based on individualistic and utilitarian premises.
3. *Conservative ethicists* oppose human enhancement, defending a concept of human beings that is embedded in the order of nature or a religious context
4. Questioning technological perfection by humans, the *sceptic* holds a critical view on technological developments, in general.

The beliefs and convictions of scientists play a highly important role in shaping the development of human enhancement technologies. Contrary to humanist scholars, engineers and natural scientists, who actively participate in the research of these technologies, tend to adopt the transhumanist or liberal ethicist view. However, these positions often overlap in practice, making it difficult to categorise single academics or groups of researchers.

Despite the importance of scientists' attitudes towards human enhancement, research institutions dealing with BCIs or neuro-enhancing pharmaceuticals are often closely connected to companies with commercial interests in the same field. In addition to financing research and drawing on informal contacts, the private sector has a huge impact on setting the agenda for researchers, especially in applied sciences. Moreover, due to the relative novelty and high dynamic in the field of BCI technologies and neuro-enhancers, the role of spin-offs, promoted by most research universities and institutes, should not be underestimated.

Users

An often neglected group of stakeholders are the users and potential consumers.[923] Regardless of developers, manufacturers and suppliers, the customers at the end of the supply chain play a crucial role by creating demand. In the context of BCI technology and neuro-enhancers, users can be categorised as "enhancement customers" and patients. Although extremely difficult, as already pointed out, the distinction is relevant in relation to the assessment of the relative value placed upon privacy and data protection. In the case of BCI applications, locked-in patients, for instance, probably have a totally different perception of the value of their privacy, including the control over their personal data, than the BCI gamer might have. In general, patients' *willingness-to-sacrifice* not only in material terms but also concerning their bodily privacy or release of sensitive data can be expected to be much greater than that of someone who pursues enhancement. However, since the lines between healthiness and illness/handicap are blurred, the level of suffering of a seemingly healthy person could be equally as high as that of somebody considered ill. The same applies to consumers of neuro-enhancers.

7.3 RISKS TO DATA PROTECTION AND PRIVACY

7.3.1 Different impacts on data protection and privacy

Data protection and privacy are differently affected by pharmacological and technical enhancement.[924] Whereas data protection is only touched upon when there is a human enhance-

[923] Oudshoorn, Nelly, and Trevor Pinch (eds.), *How Users Matter: The Co-Construction of Users and Technology*, MIT Press, Cambridge, MA and London, 2003.
[924] For a more comprehensive and encompassing theoretical discussion on differences between the concepts of privacy and data protection see Gutwirth, Serge, Raphael Gellert, Rocco Bellanova, Michael Friedewald, Philip Schütz, David Wright, Emilio Mordini and Silvia Venier, *Legal, Social, Economic and Ethical Conceptualisa-*

ment technology involved that is capable of collecting data regardless of how it may be further processed, privacy is often jeopardised when the method of enhancement implies the internalisation of substances or technologies (bodily privacy) and/or a potential loss of control.

BCI technology is able to collect highly sensitive personal data.[925] The quality of this data is comparable to genetic information, since the images created by the brain's electrical impulses have an enormous depth of information about the individual, his/her mind and way of thinking. "For the first time it may be possible to breach the privacy of the human mind, and judge people not only by their actions, but also by their thoughts and predilections."[926] Another similarity between DNA and BCI data is the fact that, even today, nobody can realistically anticipate what kind of sensitive information could be extracted from the data in the future.[927]

Yet, BCIs are, in a lot of instances, not originally designed to extract data from the carrier of the technology. There are application areas such as *neuromarketing*, which concentrate on the systematic collection, storage and processing of data concerning the brain activity of probands confronted with brand products, but most BCIs today are meant to support people in communication or control of other technology. Because BCIs are controlled by electrical impulses from the brain and no neuromuscular activity is needed, they enable partially or fully paralysed people suffering from neuromuscular diseases, such as amyotrophic lateral sclerosis (ALS), brain(stem) strokes, cerebral palsy or spinal injuries, to communicate and regain at least a bit of control over their lives. Potential forms of applications would be the mental typewriter as well as brain-to-robot interfaces. Here, the aforementioned patients' greater willingness-to-sacrifice must be critically reflected, resulting in an often distorted idea and perception of privacy.[928]

Since the latest BCI technology is based on learning processes on both sides (human and machine), manipulation of the BCI carrier could be possible as well.[929] The gain in control could then easily result in a loss of the same, confronting the user with unintended and potentially devastating consequences, especially if individuals really depend on the technology linked to the BCI.[930]

---

tions of Privacy and Data Protection, PRESCIENT: Privacy and Emerging Fields of Science and Technology: Towards a Common Framework for Privacy and Ethical Assessment, Deliverable D1, Fraunhofer ISI, Karlsruhe, 2011.

[925] Although BCI data could be seen as health data, which is considered sensitive and thus particularly protected from unauthorised access by instruments such as *informed consent*, legal clarification and/or specific legal stipulations are missing.

[926] Farah, Martha J., "Neuroethics: The practical and the philosophical", *Trends in Cognitive Sciences*, Vol. 9, No. 1, 2005, pp. 34-40 [p. 34].

[927] Despite this problematic legal situation, secure systems, as with the early days of the Internet, were apparently given little thought, when researchers developed the technical infrastructure of BCIs. That way hacker can easily attack BCIs, as shown at the US Medical Device Security Center in Massachusetts.
(cf. Bell, Vaughan, "25 ideas for 2010: Neurosecurity", *Wired UK*, 2 Nov 2009. http://www.wired.co.uk/magazine/archive/2009/12/features/25-ideas-for-2010-neurosecurity,).

[928] Since privacy is in its value to the individual and society not absolute, reconciliation with other values and interests such as the patient's wish for treatment and cure must not be forgotten. However, particularly patients' privacy seems to be at stake when the balancing implies a trade-off.

[929] McFarland and Wolpaw, op. cit., 2011, p. 63.

[930] This is particularly true in the case of CBIs such as deep brain stimulation, in which patients suffering from severe diseases, e.g. Parkinson's, are confronted with side effects such as a change in their personality. Even though most of the CBIs today are linked to medical fields of applications and fall therefore out of the concept of

Although brain imaging is at best a rough measure of personality (not to say it is uninformative even in its current state of development), "the public tends to view brain scans as more accurate and objective than in fact they are."[931] Pushed by new research opportunities through BCI technologies, behavioural neuroscience is now capable of locating parts of the brain that are supposed to be responsible for certain kinds of behaviour, attitudes and actions. That way, not only would the anticipation of buying behaviour be possible, but preventive strategies, for example in law enforcement, could also be forced upon individuals.[932]

In the case of pharmaceutical neuro-enhancement, data protection issues are not affected. Instead, neuro-enhancers are problematic in relation to the concept of bodily privacy (privacy of the person) and autonomy.[933] Although they represent a softer way of invading one's body in comparison with the implantation of technology, their bio-chemical effects take place inside the human body. Furthermore, they not only provide users with potential mental or emotional enhancement, but are also closely linked to the risk of losing control over one's will and actions. That is why specially prescribed enhancement drugs such as Ritalin or modafinil pose the threat of external control (heteronomy) by physicians, parents, employers, etc. over the individual. In addition, neuro-enhancers have successfully entered the mass market, as opposed to BCI technology, and can thus be considered to already be having a major impact on today's society.[934] Aldous Huxely contributes to this discussion in his famous novel *Brave New World*. He creates a totalitarian system that is, *inter alia*, based on a freely distributed drug called *Soma*, providing not only happiness and joy for the citizens, but also an indifferent and docile attitude towards the state.

The following figure assesses the impact of the discussed human enhancement technologies and pharmaceuticals on data protection and privacy. The two axes visualise the intensity of potential infringements.

---

human enhancement, prospective enhancement usages and deployments such as the augmentation of mental capacity by adding memory or upgrading processing power, are possible.

[931] Farah, op. cit., 2005, p. 35.

[932] Kepecs, op. cit., . 2011.

[933] Cf.: Table of types of privacy in this deliverable.

[934] Eckhardt, et al., op. cit., 2011, p. 18.

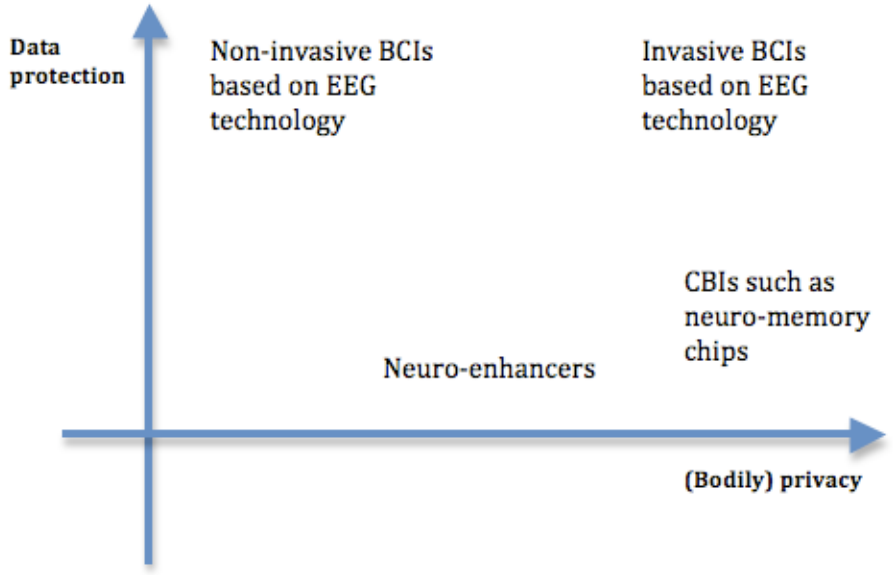


Figure 7.4: Differences in human enhancement's impact on privacy and data protection

Since one central element of human enhancement is the internalisation of technology or biochemical substances into the human body, a core sphere of privacy, i.e. bodily privacy, is almost always affected. However, privacy is to a certain extent a subjective and context-dependent notion. Hence, there will frequently be individuals who are not concerned about such intrusions and who pursue human enhancement regardless of any privacy-invasive consequences. These individuals may either be exceptions comprising a footnote in history, or represent pioneers who shape future trends in society.[935]

Nonetheless, it seems that concepts of privacy such as Warren and Brandeis' *the right to be left alone*,[936] Westin's *informational privacy*,[937] the need to have control over one's will, thoughts and body, as well as Nissenbaum's *privacy as contextual integrity*[938] continue to reflect the mainstream view of the majority of citizens in most Western societies.

Next to the typology of privacy infringements in the PRESCIENT project (cf. chapter 9), Kasper's classification of privacy invasions is very helpful in distinguishing the different dimensions and nuances of data protection and privacy affected by the discussed methods of human enhancement.[939] Although not necessarily related to data, i.e. the technical (today often digitalised) processing (collection, storage, exchange and use) of information, her *extraction type of privacy invasion* mainly refers to Westin's dimension of informational privacy. *Observation* is also linked to this concept. Since BCIs are capable of collecting and processing personal data, extraction and even real-time observation is possible. Due to the high

[935] Experimenting with RFID and later neuronal implants on himself, Kevin Warwick who is a professor of cybernetics at the University of Reading, UK, can be seen as such a person. Cf.: Haggerty, Kevin D., and Richard V. Ericson, "The surveillant assemblage", *British Journal of Sociology*, Vol. 51, 2000, pp. 605-622. http://doi.wiley.com/10.1080/00071310020015280

[936] Warren, Samuel, and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5, 15 Dec 1890, pp. 193-220.

[937] Westin, Alan, *Privacy and freedom*, Atheneum, New York, 1967.

[938] Nissenbaum, Helen, "Privacy as contextual integrity", *Washington Law Review*, Vol. 79, No. 1, Feb 2004, pp. 101-139.

[939] Kasper, Debbie V. S., "The Evolution (or Devolution) of Privacy", *Sociological Forum*, Vol. 20, No. 1, 2005, pp. 69-92 [pp. 75]. http://doi.wiley.com/10.1007/s11206-005-1898-z

quality of the data, the data processor is, in fact, able to gain information from the data subject not only about his/her communication, e.g. in the case of the mental typewriter, but also concerning more complex facts such as his/her inner-state and behaviour.

Kasper's *intrusion type of privacy invasion* is linked to the refusal of the "privacy subject", contradicting, at least to a certain extent, the concept of human enhancement, which often seems to be characterised by voluntary action. However, considering the perception of privacy as a highly fluent and dynamic concept, even from an individual point of view, it could be possible that the attitude of the user/consumer towards the human enhancement technology/pharmaceutical changes over time, leading it to become perceived as an unwanted intrusion he/she may even come to depend upon. BCI technology as well as neuro-enhancing pharmaceuticals, both qualify as this third type of privacy invasion. Although coercion and manipulation of the individual is not part of the original idea of human enhancement, it could be a consequence of being subject to enhancement technologies or pharmaceuticals.

7.3.2 Different levels of data protection

In order to understand the changing nature and quality of personal data, it is enlightening to take a closer look at the development of ICTs in recent decades, their processing data capabilities and corresponding data protection legislations. According to the German legal scholar Alexander Roßnagel, there have been three seminal stages of technological development relevant to the quantity and quality of processing personal data:[940]

1. The first urge to protect personal data arose from the worldwide launch of centralised data processing in large computer centres. This period was characterised by manual data input, data processing only in specific, rather rare situations, and a rather clear and assessable quantity of collected personal data. Roßnagel is of the opinion that data protection legislation up until today has remained on that regulatory level, meaning that the design of data protection provisions, even nowadays, has always been directed towards this centralised ICT stage. [941]
2. Afterwards, the worldwide cross-linking of PCs became the basic prerequisite for the development of a new virtual social space. Almost every activity in the real world was now possible on the Internet. However, being online leaves traces, which led to the result that, neither the spreading, nor the usage of disseminated personal data was any longer controllable.
3. Since then, the next big step has often been described as ubiquitous computing, i.e. the diffusion of data processing capabilities to objects in everyday life. That way, the physical and the virtual world are becoming increasingly interconnected. There seems to be no way to control the collection and dissemination of personal data in the two realms, because every sphere of life is potentially affected, making it almost impossible to avoid the virtual world.

Human enhancement technologies that are capable of collecting data, such as BCIs or ICT implants, could comprise a fourth stage, not only fundamentally changing the nature of personal data, but also revolutionising the intensity of cross-linking. BCIs are already generating

[940] Roßnagel, Alexander, "Datenschutz im 21. Jahrhundert", *Aus Politik und Zeitgeschichte*, Vol. 5-6, 2006, pp. 9-15 [p. 9].
[941] Another stage that Roßnagel seems to skip is the so-called *computational turn*, which is marked by the introduction of the Personal Computer and the following decentralisation of computers.

an unprecedented quality of personal data opening up new opportunities for exploitation, e.g. neuro-marketing. The implantation of BCIs or ICTs in the human body would furthermore not only let the link between virtual and real world become complete, but would also make perfect control and a panoptic society in its ideal state possible, since, for example, IP-addresses would no longer be associated with a certain technical device, but could be linked to a natural person.

7.4 REGULATION STRATEGIES

Unlike in ethics, legal research has mostly been evading a comprehensive and systematic assessment of human enhancement.[942] However, the regulatory landscape for BCIs and neuro-enhancers could not to be more different. Whereas the first are characterised by the absence of any specific regulatory approaches, the second are subject to a broad spectrum of regulations.

Contrary to some neuro-enhancers such as Ritalin, BCI technology is relatively new and not that wide-spread in the market. That is why the public, politicians and even data protection authorities have not yet seen the necessity for effective regulation. Of particular importance is the fact that the classification (or whether at all) of BCI data as sensitive (health) data is still not clear, which could lead to its misuse and extensive commercial exploitation.

The European Group on Ethics in Science and New Technologies (EGE) has issued an opinion to the European Commission in 2005 on ethical aspects of ICT implants in the human body. The EGE comes to the conclusion that, inter alia, the reviewed field of ICT implants needs regulation:

> Currently, non-medical ICT implants in the human body are not explicitly covered by existing legislation, particularly in terms of privacy and data protection. Any regulations need to be based on the following principles: dignity, human rights, equity, autonomy and the derived principles, precautionary, data minimisation, purpose specification, proportionality and relevance.[943]

However, the EGE has not considered the special nature of BCI data or non-invasive BCIs, which are, in fact, the more prevalent form of the technology. Interestingly, the EGE eventually suggests that "implantable devices for medical purposes should be regulated in the same way as drugs when the medical goal is the same".[944] This recommendation coincides with the practice that health care laws often provide an important point of reference to the assessment and evaluation of clear therapeutic BCI applications.

There are other single initiatives by research institutions such as the Medical Device Security Center (MDSC) at the University of Massachusetts Amherst, where researchers are focusing on the new field of "neurosecurity".[945]

However, particularly non-invasive BCI technologies and associated data are not subject to any specific laws, self-regulation or privacy-by-design approaches. Thus, fundamental rights, ethical guidelines as well as societal norms and moral values provide the only frameworks for indirect regulatory and judicial review opportunities.

---

[942] Eckhardt, et al., op. cit., 2011, p. 191.
[943] Rodotà, Stefano, and Rafael Capurro, "Ethical Aspects of ICT Implants in the Human Body", European Group on Ethics in Science and new Technologies (EGE), European Commission, 2005, p. 35.
[944] ibid.
[945] Medical Device Security Center, "Medical Device Security Center", 2011. http://secure-medicine.org/

Since there is an enormous variety of illegal and legal neuro-enhancing pharmaceuticals, different regulatory frameworks have to be taken into account. Concerning the regulation of illegal neuro-enhancers such as amphetamines, international narcotics conventions and national narcotics laws are certainly among the most relevant forms of regulation.[946] Neuro-enhancers that are only available on prescription, e.g. Ritalin, but also OTC drugs are subject to pharmaceutical legislation such as the German Medicinal Product Act or Medicines Act in the UK. However, none of these drug regulations considers potential privacy infringements in terms of the physical integrity of the user or external control of a third party.

Since the term "human enhancement" is not only highly contested, but also comprises a variety of entirely different technologies and pharmaceuticals, a holistic regulatory approach would miss the target. Instead, sectoral regulation would seem appropriate, augmented by effective monitoring of institutions such as ethical commissions, which uphold and orientate themselves and their evaluations around fundamental rights such as human dignity, free will, and the right to privacy and protection of personal data.[947]

7.5 CONCLUSION

This case study has dealt with technical and pharmacological human enhancement in light of current concepts of privacy and data protection. Since the term *human enhancement* is highly contested and difficult to define, the first section isolated, outlined and explored central features. The most distinguishable attributes that regularly emerged in relevant literature were:

1. Artificial (socially controversial)
2. Internal (within the human body)
3. Non-therapeutic (no medical application)

The three attributes have to be seen as an approximation of what is actually meant by human enhancement. Today, virtually no technology fulfils every feature. Instead, the technologies and pharmaceutical substances that have been analysed in this case study possess single enhancement characteristics.

Brain computer interfaces (BCIs) have been selected to serve as an example of technology with human enhancement features. The most important categorisations of BCIs in relation to their privacy invasiveness, are their location (invasive vs. non-invasive) as well as their direction of operation (from human to machine and/or vice versa). Although the latter can be found in forms of medical applications such as deep brain stimulation, most BCI technology is used to image brain activity. Measuring the electrical impulses emitted by the brain, electroencephalography (EEG) is the most prevalent method of displaying brain activity. Although applications such as the mental typewriter or brain-to-robot interfaces are, at the moment, primarily developed for therapeutic purposes, the gaming and entertainment industry has recently shown an increased interest in BCI technology.

Neuro-enhancing pharmaceuticals (neuro-enhancers) constitute the second part of the case study. Characterised by its biological and chemical effects, pharmaceutical neuro-enhancement comprises not only illegal drugs (amphetamine or cocaine), but also legal medical products, i.e. either available on prescription (off-label use is possible), e.g. antidepres-

[946] The term *narcotic drug* refers only to the prohibited/illegal status of the drug, not revealing any information about its effects on health or addictiveness.

[947] A more comprehensive but rather generic legal analysis is conducted by VUB in one of the following chapters.

sants and methylphenidate (Ritalin), or OTC (over-the-counter) drugs such as aspirin. Since the off-label usage of Ritalin is particularly extensive, it serves as an example that is also discussed in terms of its privacy-invasive potentials.

Data protection and privacy are affected in different ways by pharmacological and technical enhancement. Whereas data protection is only touched upon when there is a human enhancement technology involved that is capable of collecting data regardless of how it may be further processed, privacy is often at risk when the method of enhancement implies the internalisation of substances/technologies (bodily privacy) and/or a potential loss of control.

BCI technology is above all able to collect highly sensitive personal data. The quality of this data is comparable to genetic information, since the images created by the brain's electrical impulses have an enormous depth of information about the individual, his/her mind and way of thinking. In addition, nobody can realistically anticipate what kind of sensitive information may be extracted from the data in the future. However, clear legal provisions or guidance determining the sensitive character of BCI data, according to the EU Data Protection Directive Article 8, does not yet exist. This is particularly problematic, since more and more ways of commercialising BCI data are emerging. Despite this problematic legal situation, secure systems, similar to the early days of the Internet, were apparently given little thought when researchers developed the technical infrastructure of BCIs. Thus, hackers can easily attack BCIs, as shown at the Medical Device Security Center. Beyond data protection, privacy issues are particularly engaged, when brain-imaging processes are invasive or inverted, i.e. the brain is given an external electrical input. This is the case for CBIs such as deep brain stimulation.

Concerning pharmaceutical neuro-enhancement, data protection issues are not affected. Instead, neuro-enhancers are problematic in relation to the concept of bodily privacy and individual autonomy. Although they represent a softer form of invading one's body in comparison with the implantation of technology, their bio-chemical effects still take place inside the human body. Furthermore, the taking of neuro-enhancing drugs can result in the risk of losing control over one's will and actions, Therefore, specially prescribed enhancement drugs such as Ritalin pose the threat of external control by physicians, parents, employers, etc. In addition, neuro-enhancers have successfully entered the mass market, as opposed to BCI technology, and can thus be considered to already be having a major impact on today's society.

Since one central element of human enhancement is the internalisation of technology or bio-chemical substances into the human body, a core sphere of privacy, i.e. bodily privacy, is almost always affected. However, privacy is to a certain extent a subjective and context-dependent notion. Hence, there will frequently be individuals who disregard privacy concerns, pursuing human enhancement regardless of any privacy-invasive consequences.

7.6 REFERENCES

Al-Sagban, Mariam, Omnia El-Halawani, Tasneem Lulu, et al., "Brain Computer Interface as a Forensic Tool", in *5th International Symposium on Mechatronics and Its Applications*, IEEE, Amman, 27-29, May 2008.

Allhoff, Fritz, Patrick Lin, James Moor and John Weckert, *Ethics of Human Enhancement: 25 Questions & Answers*, Report prepared for the US National Science Foundation under awards # 0620694 and 0621021, Human Enhancement Ethics Group, 2009.

Andler, Daniel, Simon Barthelmé, Bernd Beckert, et al., *Converging technologies and their impact on the social sciences and humanities (CONTECS): An Analysis of critical*

issues and a suggestion for a future research agenda, Final Report, 2008. http://www.contecs.fraunhofer.de/

Baranski, Joseph V., Ross Pigeau, Peter Dinich and Ira Jacobs, "Effects of modafinil on cognitive and meta-cognitive performance", *Human Psychopharmacology: Clinical and Experimental*, Vol. 19, No. 2004, pp. 323-332. http://doi.wiley.com/10.1002/hup.596

Beckert, Bernd, Clemens Blümel and Michael Friedewald, "Visions and Realities in Converging Technologies: Exploring the technology base for convergence", *Innovation - The European Journal of Social Science Research*, Vol. 20, No. 4, 2007, pp. 375-394.

Beckert, Bernd, Bruno Gransche and Philine Warnke, *Mensch-Technik-Grenzverschiebung - Perspektiven für ein neues Forschungsfeld*, Fraunhofer Verlag, Stuttgart, 2011.

Bell, Vaughan, "25 ideas for 2010: Neurosecurity", *Wired UK*, 2 Nov 2009, http://www.wired.co.uk/magazine/archive/2009/12/features/25-ideas-for-2010-neurosecurity.

Coenen, Christopher, "Utopian Aspects of the Debate on Converging Technologies", in Banse, Gerhard, Imre Hronszky, et al. (eds.), *Converging Technologies. Promises and Challenges*, Sigma, Berlin, 2007.

Coenen, Christopher, Stefan Gammel, Reinhard Heil and Andreas Woyke (eds.), *Die Debatte über "Human Enhancement": Historische, philosophische und ethische Aspekte der technologischen Verbesserung des Menschen*, Transcript Verlag, Bielefeld, 2010.

Cuhls, Kerstin, Walter Ganz, Philine Warnke, et al., "Foresight-Prozess im Auftrag des BMBF: Zukunftsfelder neuen Zuschnitts", Fraunhofer ISI, Fraunhofer IAO, Karlsruhe/Stuttgart, 2009.

DAK, "Gesundheitreport 2009. Analyse der Arbeitsunfähigkeitsdaten. Schwerpunktthema Doping am Arbeitsplatz. Deutsche Angestellten Krankenversicherung", Deutsche Angestellten Krankenversicherung, 2009.

Dunbar, Graham, "Double-amputee wins appeal to aim for Olympics", *The Independent*, 16 May 2008, http://www.independent.co.uk/sport/general/athletics/doubleamputee-wins-appeal-to-aim-for-olympics-829647.html

Eckhardt, Anne, Andreas Bachmann, Michèle Marti, et al., *Human Enhancement* vdf Hochschulverlag, Zürich, 2011.

Editorial, "Brain scam?", *Nature Neuroscience*, Vol. 7, No. 7, 2004, pp. 683.

Evers, Kathinka, "Perspectives on Memory Manipulation: Using Beta-Blockers to Cure Post-Traumatic Stress Disorder", *Cambridge Quarterly of Healthcare Ethics*, Vol. 16, No. 2, 2007, pp. 138-146. http://www.journals.cambridge.org/abstract_S0963180107070168

Farah, Martha J., "Neuroethics: The practical and the philosophical", *Trends in Cognitive Sciences*, Vol. 9, No. 1, 2005, pp. 34-40.

Frean, Alexandra, and Patrick Foster, " Cheating students turn to smart drug for edge in exams", *The Sunday Times*, 23 Jun 2007,

Gehlen, Arnold, *Die Seele im technischen Zeitalter. Und andere soziologische Schriften und Kulturanalysen [1957]*, Vittorio Klostermann, Frankfurt, 2004.

Gerlinger, Katrin, Thomas Petermann and Arnold Sauter, *Gendoping: Wissenschaftliche Grundlagen, Einfallstore, Kontrolle*, Edition Sigma, Berlin, 2008.

van Gerven, Marcel, Jason Farquhar, Rebecca Schaefer, et al., "The brain–computer interface cycle", *Journal of Neural Engineering*, Vol. 6, No. 4, 2009, pp. 1-10.

Gransche, Bruno, *Der Mensch als Autofakt: Technik-Haben und Technik-Sein in der New Reality des 21. Jahrhunderts*, VDM Verlag Dr. Müller, Saarbrücken, 2010.

Grunwald, Armin, "Converging Technologies for Human Enhancement: A New Wave Increasing the Contigency of the conditio humana", in Gerhard Banse and Armin Grunwald et al. (eds.), *Assessing Societal Implications of Converging Technological Development*, Edition Sigma, Berlin, 2007, pp. 271-288.

Gutwirth, Serge, Raphael Gellert, Rocco Bellanova, Michael Friedewald, Philip Schütz, David Wright, Emilio Mordini, and Silvia Venier, *Legal, Social, Economic and Ethical Conceptualisations of Privacy and Data Protection*, PRESCIENT: Privacy and Emerging Fields of Science and Technology: Towards a Common Framework for Privacy and Ethical Assessment: Deliverable D1, Fraunhofer ISI, Karlsruhe, 2011.

Haggerty, Kevin D., and Richard V. Ericson, "The surveillant assemblage", *British Journal of Sociology*, Vol. 51, No. 2000, pp. 605-622. http://doi.wiley.com/10.1080/00071310020015280

Hüsing, Bärbel, L. Jäncke and B. Tag, *Impact Assessment of Neuroimaging*, IOS Press, Amsterdam, 2006.

Kasper, Debbie V. S., "The Evolution (or Devolution) of Privacy", *Sociological Forum*, Vol. 20, No. 1, 2005, pp. 69-92. http://doi.wiley.com/10.1007/s11206-005-1898-z

Kepecs, Adam, "Neuroscience: My brain made me do it", *Nature*, Vol. 473, No. 2011, pp. 280-281. http://www.nature.com/doifinder/10.1038/473280a

Knight, Tom, "IAAF call time on Oscar Pistorius' dream", *Telegraph*, 10 January 2008. http://www.telegraph.co.uk/sport/othersports/athletics/2288489/IAAF-call-time-on-Oscar-Pistorius-dream.html

Krepki, Roman, Gabriel Curio, Benjamin Blankertz and Klaus-Robert Müller, "Berlin Brain–Computer Interface—The HCI communication channel for discovery", *International Journal of Human-Computer Studies*, Vol. 65, No. 5, 2007, pp. 460-477.

Longman, Jeré, "An Amputee Sprinter: Is He Disabled or Too-Abled?", *New York Times*, 15 May 2007. http://www.nytimes.com/2007/05/15/sports/othersports/15runner.html?_r=1&oref=slogin

Maguire, G. Q., and Ellen M. McGee, "Implantable Brain Chips? Time for Debate", *The Hastings Center Report*, Vol. 29, No. 1, 1999, pp. 7-13. http://www.jstor.org/stable/3528533

McFarland, Dennis J., and Jonathan R. Wolpaw, "Brain-computer interfaces for communication and control", *Communications of the ACM*, Vol. 54, No. 5, 2011, pp. 60-66.

Moore, Karl, "Maybe it is like brain surgery: How neuromarketing is using brain scan technologies to give new insights into the "black box" of the consumer mind", *Marketing Magazine*, Vol. 110, No. 14, 2005, pp. 12.

Nijholt, Anton, "BCI for Games: A 'State of the Art' Survey", in Scott M.Stevens and Shirley J. Saldamarco (eds.), *Entertainment Computing - ICEC 2008*, Springer, Berlin Heidelberg, 2009, pp. 225-228. http://www.springerlink.com/index/10.1007/978-3-540-89222-9_29

Nissenbaum, Helen, "Privacy as Contextual Integrity", *Washington Law Review*, Vol. 79, No. 1, 2004, pp. 101-139.

Nordmann, Alfred, "Converging Technologies - Shaping the Future of European Societies", EUR 21357, Office for Official Publications of the European Communities, Luxembourg, 2004.

Novartis, *Novartis erzielt 2009 Rekordergebnisse - Neu eingeführte Produkte erweisen sich als Wachstumstreiber*, Financial Report, Basel, 2010.

Ortiz Jr., Sixto, "Brain-Computer Interfaces: Where Human and Machine Meet", *IEEE Computer*, Vol. 40, No. 1, 2007, pp. 17-21.

Oudshoorn, Nelly, and Trevor Pinch (eds.), *How Users Matter: The Co-Construction of Users and Technology*, MIT Press, Cambridge, MA and London, 2003.

Raabe, Kristin, "Stimulieren ohne Nebenwirkungen", *Technology Review (Deutsche Ausgabe)*, Vol. 8, No. 2011, pp. 10-11.

Repantis, Dimitris, "Die Wirkung von Psychopharmaka bei Gesunden", in Wienke, Albrecht, Wolfram Eberbach, et al. (eds.), *Die Verbesserung des Menschen*, Springer, Berlin, Heidelberg, 2009, pp. 63-68. http://www.springerlink.com/index/10.1007/978-3-642-00883-2_5

Reschke, Stefan, "Verbesserung menschlicher Leistungsfähigkeit", in Fraunhofer INT (ed.), *Jahresbericht 2009*, Fraunhofer-Institut für naturwissenschaftlich-technische Trendanalysen, Euskirchen, 2010, pp. 18-19.

Roco, Mihail C., and William Sims Bainbridge (eds.), *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science*, Kluwer, Dordrecht, 2003.

Rodotà, Stefano, and Rafael Capurro, "Ethical Aspects of ICT Implants in the Human Body", European Group on Ethics in Science and new Technologies (EGE), European Commission, 2005.

Roßnagel, Alexander, "Datenschutz im 21. Jahrhundert", *Aus Politik und Zeitgeschichte*, No. 5-6, 2006, pp. 9-15.

Science and Technology Options Assessment (STOA), "Human Enhancement Study", European Parliament, 2009.

Science and Technology Options Assessment (STOA), "Making Perfect Life: Bio-engineering (in) the 21st Century", European Parliament, 2011.

Theißen, Sascha, *Risiken informations- und kommunikationstechnischer (IKT-) Implantate im Hinblick auf Datenschutz und Datensicherheit*, Universitätsverlag Karlsruhe, Karlsruhe, 2009.

Thorpe, Julie, P. C. van Oorschot and Anil Somayaji, "Pass-thoughts", in *Proceedings of the 2005 workshop on New security paradigms (NSPW 05)*, ACM Press, 2005, pp. 1-11. http://portal.acm.org/citation.cfm?doid=1146269.1146282

U.S. President's Council on Bioethics, "Beyond Therapy - Biotechnology and the Pursuit of Happiness", 2003.

Vidal, Jacques J., "Toward direct brain-computer communication", *Annual review of Biophysics and Bioengineering*, Vol. 2, No. 1, 1973, pp. 157–180.

Warren, Samuel, and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5, 15 Dec 1890, pp. 193-220.

Westin, Alan, *Privacy and freedom*, Atheneum, New York, 1967.

Woyke, Andreas, "Human Enhancement und seine Bewertung – Eine kleine Skizze", in Coenen, Christopher, Stefan Gammel, et al. (eds.), *Die Debatte über "Human Enhancement": Historische, philosophische und ethische Aspekte der technologischen Verbesserung des Menschen*, Transcript Verlag, Bielefeld, 2010, pp. 21-40.

Yahud, Shuhaida, and Noor Azuan Abu Osman, "Prosthetic Hand for the Brain-computer Interface System", in Ibrahim, Fatimah, Noor Azuan Abu Osman, et al. (eds.), *3rd Kuala Lumpur International Conference on Biomedical Engineering 2006*, Springer, Berlin, Heidelberg, 2007, pp. 643-646. http://www.springerlink.com/index/10.1007/978-3-540-68017-8_162

Chapter 8, Legal Uncertainties

Raphaël Gellert and Serge Gutwirth
Vrije Universiteit Brussel

8.1 METHODOLOGICAL REMARKS

The goal of this task is to identify the legal uncertainties stemming from the technologies described earlier on in the deliverable with regards to privacy and data protection. In other words, the aim is to determine the lawfulness of these practices with regards to data protection and privacy principles.

As far as privacy is concerned, we will refer to the test contained in articles 8.2 ECHR and 52.1 CFR, which require, in addition to a legitimate aim, that the interference be provided for by the law, be proportional to the aim pursued and be necessary in a democratic society.

For an exception to be 'provided by the law', several conditions must be met. First, the impugned measure should have some *basis in domestic law*. Second, the law in question should be *accessible* to the person concerned. Third, the person *must be able to foresee its consequences*. Fourth, the law must be *compatible with the rule of law*. Finally, the measure must *comply with the requirements* laid down by the domestic law providing for the interference.[948]

The condition of *necessity* can be divided in three sub-conditions.

(1) The necessity shall be justified by 'a *pressing social need'*,
(2) The interference must be *proportionate* to the legitimate aim pursued,
(3) The reasons put forth by the national authorities to justify it shall be '*relevant and sufficient'*.[949]

This last requirement is also known as the proportionality or "balancing" test. In the previous deliverable (D.1), we have determined what constitutes, according to us, a sound proportionality test. In a nutshell, a strong proportionality test should not be limited to weighting one value (or right) against the other, but should include the possibility of determining whether the measure is strictly "necessary in a democratic society", which entails that if the proposed measure harms the essence of a fundamental right or of the constitutional order, although it effectively realizes the legitimate aim pursued, it shall be deemed as unlawful. Finally, a last aspect of a strong proportionality test consists in the obligation to explore if there are alternative measures that allow for the realisation of the legitimate interest, but that do not affect the fundamental rights in the same way as the proposed measure, i.e., to look for less (constitutionally) harmful solutions.[950]

As explained in the first deliverable the right to data protection is different from the right to privacy: it is constructed as a set of "Fair Information Practices". Consequently, any violation of one of these practices equates to a violation of the right.[951] However, data protection en-

---

[948] Els, Kindt, and Müller, Lorenz, "D13.4: The privacy legal framework for biometrics", FIDIS - Future of Identity in the Information Society, 2009, p. 17. Available on the following website, http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis_deliverable13_4_v_1.1.pdf; See also De Hert, Paul, and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg", *in* Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwagne, Sjaak Nouwt (eds.), *Reinventing Data Protection?* , Doordrecht: Springer, 2009, pp. 20-23.

[949] Kindt & Müller, 2009, p. 18.

[950] See, Gutwirth, Serge, Raphael Gellert, Rocco Bellanova, Michael Friedewald, Philip Schütz, David Wright, Emilio Mordini, and Silvia Venier, Deliverable D.1: Legal, social, economic and ethical conceptualisations of privacy and data protection, *PRESCIENT: Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment*, 2011, pp. 27-28.

[951] Ibidem, p. 5.

compasses different types of provisions. Whereas some grant data subjects a set of subjective rights, others determine the criteria a processing of data should meet. They are contained in article 6 (the principles) and 7 (the legitimacy grounds) of Directive 95/46/EC.[952]

Article 6 1 (b) of the Directive 95/46/EC (also known as the data protection Directive) requires that data must be collected for specified, explicit and legitimate purposes and that they shall not be processed in a way incompatible with those purposes. It enshrines the so-called **purpose specification principle** (also referred to as PSP in the text) that aims at setting the limits within which personal data may be processed. It also determines how and to what extent data collected for one purpose (which must be legitimate according to article 7) may be used for other purposes. This principle prohibits further processing for a purpose that differs from the original one that justified in the first instance the processing of data. Consequently, data should be kept for no longer than is necessary for the purpose for which it was first collected.[953] The Art.29 WP has qualified this last principle as the conservation principle.[954]

According to the **data quality principle**, the personal data processed, must be adequate, relevant and not excessive in relation to the purpose pursued. Thus, any irrelevant data must not be collected, and if it has been collected it must be discarded.[955] Also, data processed must be accurate and kept up-to date.[956]

When coupled together these two principles can be coined as the **data minimisation** principles, which states that the processing of data must be proportionate (cf. data quality requirements), and must be undertaken if and only if, it appears as strictly necessary in order to achieve a determinate purpose (purpose specification).[957] The idea is that the aim of the processing should be attained by the processing of, as less as possible personal data.

8.2 WHOLE GENOME SEQUENCING

8.2.1 The nature of genetic data, and the ensuing consequences for the applicability of the data protection Directive and the ECHR

Whole genome sequencing deals with DNA, which is considered to be genetic data.[958] As a genetic data, it is beyond doubt that it constitutes personal information and that the data protection directive is applicable.[959] As genetic data, DNA also constitutes sensitive data in the meaning of article 8 of the Directive,[960] as it reveals the health of the data subject.[961]

---

[952] As was made clear in the first deliverable, the EU Charter for Fundamental Rights, which is now binding in the EU legal order, contains a new right to the protection of personal data (article 8).
[953] Article 6 1 (e)
[954] Article 29 Working Party, Working Document on data protection issues related to RFID technology, 10107/05/EN, WP 105, Adopted on 19 January 2005, p. 9. This expression might be misleading insofar as it would suggest that data should be conserved. On the opposite, data should be conserved as little as possible.
[955] Article 6 1 (c); Art. 29, *op. cit*.
[956] Article 6 1 (d) states that personal data must be: "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."
[957] See, Gutwirth et al., 2011, p. 28; Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, 2002, pp. 95-97.
[958] See, Article 29 Data Protection Working Party, Working Document on Genetic Data, 12178/03/EN, WP 91, Adopted on 17 March 2004.
[959] **European Parliament and the Council, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.** *Official*

This of crucial importance as far as the purpose for which these data can be processed is concerned. As the Article 29 Working Party has pointed out, any use of genetic data for purposes other than directly safeguarding the data subject's health and pursuing scientific research should require national rules to be implemented.[962]

In our opinion, the fact that DNA sequencing deals with such sensitive data has an influence on the necessity, proportionality of the processing, as well as on the legitimacy of the aims pursued (cf. *supra*, Methodological remarks).[963]

For instance, article 8 of the data protection Directive lists four relevant situations for our case study whereby the processing of data is legitimate: when the data subject has given his/her explicit consent;[964] when it is required for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services;[965] when it is necessary for reasons of substantial public interest;[966] or when it is relating to offences, criminal convictions, or security measures.[967]

8.2.2 Data protection Principles

In the case study on whole genetic sequencing, there are several data processing principles that are encroached upon.

The data minimisation (thus composed of PSP and data quality), is put at jeopardy at several occasions.

Such is the case as far as **forensics** are concerned.
First is the question of how much data should be processed? Indeed, as far as now, DNA use for forensic investigations is limited to what is coined as a "DNA fingerprint", which relies

---

Journal L 281, 23/11/1995 P. 0031 – 0050. See in particular article 2 that determines the scope of the directive *ratione materiae*.

[960] Article 8.1 states that: "**Member States shall prohibit the processing** of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing **of data concerning health** or sex life" (emphasis added).

[961] Article 29 Working Party, WP 91, *loc. cit.*, p. 5.

[962] Article 29 Working Party, WP 91, *loc. cit.*, p. 13. Cf., article 8.3 of the Directive states that article 8.1 "shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy" (emphasis added).

[963] See also the case study of the European Court of Human Rights, *S. and Marprer v. The United Kingdom, 4 December 2008*.

[964] Article 8 2 (a) states that the prohibition to process sensitive data shall not apply when "*the data subject has given his explicit consent to the processing of those data*".

[965] Article 8 3 states that: "Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy."

[966] Article 8 4 states that: "Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority."

[967] Article 8 5

upon a set of 13 DNA regions. However, as whole DNA sequencing seems increasingly within reach, it might be questioned whether such a course of action would be acceptable from the perspective of data protection. Indeed, such a practice would allow not only precise individual identification but also characterisation by physical traits of the individual such as their eye, skin, hair colour and other individual characteristics (p. 14).[968] The data protection principle of data minimisation is definitely at stake here: is it proportional to use a whole human genome, is it also necessary in relation to the aim pursued? Given the risks of discovering sensitive data, one would be tempted to answer "no". Whole genomic use appears to be an excessive processing of data. Additionally, because the whole genome contains so much information it is possible to infer from it some health issues or a paternity (or any other family relationships), but not only, as it is also possible to determine the ethnicity, colour of skin etc. of the data subject.

Second, is the question of whose genetic information should be stored (i.e., sampled)?
In the case study, several options are put forward.
Comprehensive databases are clearly to be discarded. Indeed, it is by no means necessary to store everybody's DNA in order to identify criminals, let alone proportional. Furthermore, this can also lead to secondary uses that are discriminatory (e.g., refusing a job based on the DNA information). Therefore, **the violation is twofold: data are used for a secondary purpose, and this purpose is not legitimate**. It also casts a shadow of suspicion on all citizens and might lead to permanent suspicion on perfectly innocent citizens, and therefore constitutes an additional discrimination and undermines the presumption of innocence.[969]
An alternative to comprehensive databases is to sample the DNA information only of people who have been officially suspected. Although, it seems more proportional it remains disproportionate to our eyes: why should the DNA of persons merely suspected be stored in a database? There are indeed possibilities of discrimination and reversal of the presumption of innocence. One may also wonder, whether it is necessary to the identification of criminals, or if there are other, less intrusive ways to do so. As a matter of fact, the European Court of Human Rights has declared in its Marper case that keeping stored the DNA of citizens declared innocent (as well as those who were not charged) was not proportional, and thus, unlawful.[970]
Another option would be to store only the DNA of convicted criminals. It seems more justified here, especially in the light of the fact that some crimes have a high rate of recurrence and that therefore, stored DNA might facilitate crime fighting in that respect. However, such a measure has high negative impact in terms of privacy and discrimination, and thus, one can ask whether there are less intrusive ways to fight crime, and hence, whether this measure is necessary and proportional.
Furthermore, it is also important to decide for which kind of crime one wishes to store DNA. In the case of minor offences, it seems very much disproportionate.

---

[968] Yet, it can be argued that, as such, DNA-based ID data always contain more information than what is necessary for identification purposes thereby raising questions about the respect of the purpose specification principle. However, the same can be said about natural identifiers, for instance, the name of a data subject can reveal his/her ethnic origin.
[969] Gonzalez Fuster Gloria, Paul De Hert, Erika Eva Ellyne, Serge Gutwirth, "Huber, Marper and Others: Throwing new light on the shadows of suspicion", *INEX Policy Brief*, No. 11, Centre for European Policy Studies (CEPS), 2010, pp. 2-3.
[970] *S. and Marprer v. The United Kingdom, 4 December 2008*. On the case, see, De Beer, Daniel, Paul De Hert, Gloria Gonzalez Fuster, and Serge Gutwirth, « Nouveaux éclairages de la notion de «donnée personnelle» et application audacieuse du critère de proportionnalité. Cour européenne des droits de l'homme Grande Chambre S et Marper c. Royaume Uni, 4 décembre 2008 », *Revue Trimestrielle des Droits de l'Homme*, vol. 81, 2010, pp.141 – 161.

In addition to that, one needs to answer the question as to how long must the data be stored in databases. Although some claim that perpetual retention might have some virtues in crime fight, this practice raises a lot of questions, in particular with respect to the purpose specification principle, and its sub-principle, the conservation principle.

Also, it does not appear to be proportional. If one keeps in mind that storing data amounts to a processing of data, things become much more clear. Whereas it might be perfectly legitimate to process data, that is, to analyse genetic data such as DNA in the framework of a criminal investigation, the further storing instead, constitutes a problem from the point of view of data protection legislation.[971] Because, it constitutes a secondary processing, one could argue that it threatens *ipso facto* the purpose specification principle, and in particular the conservation principle. At least, this is the case in classical criminal investigation, which operates *a posteriori*.[972] However, when police forces store the genetic data, they operate *a priori*, that is, storing data not because of its current usefulness but in the belief that it could be *directly* useful and relevant in the future, in the context of the identification of criminals of crimes still to be committed.[973] This logic is totally forward-looking and demands that data be stored as long as possible.[974] However, if this is the aim pursued, one should wonder about the validity of such an aim. It clearly violates the PSP as it is well too broad to be qualified as a "specific aim". Furthermore, its legitimacy is dubious as it has clear discriminatory consequences, among which, and maybe most notably, the reversal of the presumption of innocence.

But the data minimisation principle is also put in jeopardy in the framework of scientific and medical research. Indeed, data protection texts are more permissive as far as scientific research and statistical uses are concerned, yet, not everything is allowed.
For instance, the Council of Europe recommends the use of anonymous data.[975] However, the case study described practices that involve huge numbers of participants, whose data is not only made publicly available, but also linked to the concerned individual. One has to question whether the disclosure/communication of these data is not excessive, and whether it doesn't constitute an unlawful secondary processing.
As a matter of fact, the PSP is put at jeopardy by data sharing practices. As indicated in the case study, there is a need for flexible data-sharing resources that make materials and data available with minimum restrictions on use. Ultimately, this is the problem raised by all databanks –in this case, biobanks: once the data is stored the door seems open to a multiplicity of secondary uses, thereby violating the purpose specification principle. This is all the more a problem since the data protection law, did not install a prohibitive system, but a system which is mainly based on the idea that the control of the processing of personal data can be organised through the imposed *separation* of the different processing.

In the preceding paragraphs we have evidenced ways in which the data minimisation principle is threatened. In particular, it appears to us that the potential violation of the purpose specification principle (which is a constitutive element of the former principle) leads to other challenges in terms of data protection principles. For instance, the obligation to notify the data

[971] But not only, it also remains an issue whether the keeping of such records – which nourishes a sustained suspicion - after a condemned person has undergone his/her punishment is still needed, because it is a burden for the process of social reintegration (although the latter is not a legal issue *stricto sensu*).
[972] Gonzalez Fuster et al., 2010, p. 5.
[973] Another important use, is to resolve past crimes, which were so far unsolved.
[974] *Op. cit.*, p. 5.
[975] Council of Europe, Recommendation No. 4 (83) 10 on the protection of personal data used for scientific research and statistics, 23 Septembre 1983, article 2.2.

subject of a processing of his personal information seems unsustainable as any linking, publication, or communication of genomic data would trigger this duty.[976]

As a matter of fact, and as underlined in the case study, the particular nature of genomic data also is problematic in view of the data quality principle. The latter requires that collected data must be kept up-to-date. However, keeping genomic data up-to-date is particularly problematic. As such, they are intrinsically updated, as they never change. However, our knowledge about them evolves and may lead to the discovery of new information about the genomic data. Should such information be communicated to data subjects? And what about false positive risks?

The challenges faced by the PSP (i.e., indefinite secondary uses of data) are mirrored by the problem of consent. In case the data subject's consent serves as a basis for the legitimacy of the processing (which appears to be very often the case in genomic research), how is one to constantly renew his/her consent given the infinity of processing operated concerning his/her personal information? The case study mentions some solutions that have been put forward such as "open consent". However, one may wonder if such an open configuration of consent is still meaningful, or if on the contrary, it doesn't empty the very notion of consent of its meaningfulness and thereby efficiency. One can see here analogies with forensics use of database for preventive purposes, which are too broad in order to be qualified as "specific aims" according to the PSP. The foregoing sheds some light on the limits of consent as a legitimate basis for the processing of such data. Yet, it might even be more constrained. Indeed, one may wonder if consent can **always** serve as a legitimate basis for the processing of genetic data, especially in the light of its ultra sensitive nature. In other words, is it sufficient that a citizen agrees to process his/her personal data in order to make such a processing legitimate? The case study illustrates the problematic nature of consent by touching upon issues of commercial and private use of genomic data (i.e., DTC testing, and paternity tests). Both these practices rely upon individuals' consent, yet, the case study clearly shows the risks of abuses, and the highly questionably legitimacy of such practices.
The issue of consent as a legitimate basis for the processing of personal information has been tackled in the first deliverable, wherein we asked the following question: "since articles 7 (e) and (f) do already justify any processing of personal data tending to the realisation of a legitimate aim of the processor, the legitimacy by consent criterion foreseen by art. 7 (a) will often, if not always, seem to be superfluous. So one may wonder if the consent criterion can supersede the legitimate aim criterion, which would perversely imply that consent could legitimise processing for "illegitimate aims", which indeed would be unacceptable".[977]

Furthermore, commercial processing of genomic data is problematic from another point of view: that of the sensitive nature of such data. Given, the general prohibition of article 8 of the data protection Directive, commercial processing, though backed by the data subject's consent, remains extremely dubious.

Final reflections

The sensitive nature of genomic data is such that the risks of abuses are high. Therefore, it should be very carefully assessed as to which actor can perform which action regarding those data.

[976] Article 10 and 11 of the Data Protection Directive.
[977] Gutwirth et al., 2011, p. 28.

For instance, storing data in biobanks is very risky, as the risks of secondary, and disproportionate processing are latent. If it is justifiable for medical reasons, it is not so much for forensics purposes, let alone commercial ones.
Moreover, the fact that medical research requires multiples data processing operations should lead us to rethink consent not from a quantitative viewpoint but from a qualitative perspective. This would entail that medical biobanks could perform indefinite numbers of the same type of processing, but cannot operate other types of processing (e.g., publication on website).

8.2.3 Privacy and biobanks

As a matter of fact, we have so far reasoned in terms of data protection principles precisely because data processing is crucial to this first case study. What this means, is that our analysis is valid insofar as it concerns the (fundamental) right to the protection of personal data. However, analysing the facts from the point of view of privacy might lead to other results.

In the Marper case, the ECtHR looked into the private nature of DNA and genetic data. Some of its findings are relevant for the case study at stake.

It has insisted upon the extremely private nature of these types of data. In addition to being highly personal, genetic information contains much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives.[978] In particular, it insists upon the fact that they allow the data collector to assess the likely ethnic origin of the donor, which makes their retention all the more sensitive and susceptible of affecting the right to private life.[979] Furthermore, the fact that only a limited part of this information is actually used and that no immediate detriment is caused does not change this conclusion.[980] It therefore concludes that, "given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned."[981]

Therefore, the question to be answered is whether this interference (i.e., the storage of genetic data in databases) is lawful or not. In the Marper case, which concerned police investigation, the Court declared that it was not lawful (at least according to the modalities of English police, which entailed indeterminate storage periods).[982]

Going a step further, the next question is whether there exists any storage that is lawful. We have observed that data protection rules (including Council of Europe Guidelines) are more lenient as far as the processing of personal data for medical and research purposes is concerned, provided of course it is undertaken in accordance to data protection principles. Yet, this is true only insofar as data protection is concerned. Consequently, it is not too far-fetched to make the hypothesis that, no matter what the purpose is, the storage of genetic data violates the right to privacy of individuals.

[978] *S. and Marper v. The U.K.*, 4 December 2008, § 72.
[979] Ibidem, § 76.
[980] Ibidem, § 73.
[981] Ibidem, § 73.
[982] Ibidem, § 77.

8.3 UNMANNED AIRCRAFT SYSTEMS

Some of the uses enabled by unmanned aircraft systems (UASs, i.e., devices used for flying with no on-board pilot) will be analysed in the light of data protection and privacy legislation. When used for civil purposes, the main goal of UASs is surveillance of both public and private spaces. In other words, our task is to determine the lawfulness of the new surveillance possibilities offered by UASs as far as they pertain to privacy and to data protection.

8.3.1 UASs and the right to privacy

In order to determine whether unmanned surveillance interferes with the privacy of individuals, one needs first determine whether it touches upon this very privacy.

It follows from the case study that because of its very nature, unmanned surveillance can be qualified as secret (or covert) surveillance, as in most of, if not all, the cases described, citizens are unaware of the presence of these devices.

In this respect, the ECtHr has established a solid case law according to which, "secret surveillance amounts in itself to an interference with the applicants' rights under Article 8 of the Convention".[983]
As outlined in the Deliverable D.1, privacy in the meaning of article 8 ECHR is a broad term that is not limited to the protection of an "inner circle", but also includes the right to establish and develop relationships with other human beings and the outside world, and ultimately the right to personal development.[984] Furthermore, the Court has earlier found that the systematic collection and storing of data by security services on particular individuals constituted an interference with these persons' private lives, even if that data was collected in a public place,[985] or concerned exclusively the person's professional or public activities.[986]There is privacy in the public space.
In the Perry case, the Court declared that surveillance in public premises is not concerned with the private life of individuals, unless the extent of the operation is such that it interferes with article 8 ECHR.[987] In its Uzun case, the ECtHr considered that the collection of data concerning the whereabouts and movements of a person in the public sphere through a GPS device attached this person's car constituted an interference with private life.[988]
As a result, it is not questionable that unmanned surveillance concerns the privacy of individuals.

Therefore, the question remains as to whether these operations are lawful, that is, pass the three-folded threshold test of article 8.2 of the ECHR.[989] Our analysis will focus on the conditions of legitimacy and necessity in a democratic society.

---

[983] *Association for European Integration and Human Rights and Ekimdzhev vs. Bulgaria*, 30 January 2008, § 69. See also, *Klass and Others v. Germany*, 6 September 1978, § 41; *Malone v. the U.K.*, 26 April 1985, § 64; and *Weber and Saravia v. Germany*, 2006, §§ 77-79.
[984] see *Niemietz v. Germany*, 16 December 1992, § 29, and *Halford v. the United Kingdom*, 25 June 1997, § 42-46.
[985] See, *Peck v. the U.K.*, 28 January 2003, § 59, and *P.G. and J.H. v. the U.K.*, 25 September 2001, §§ 57-59.
[986]See *Amann v. Switzerland*, 16 February 2000, §§ 65-67; and *Rotaru v. Romania*, 4 May 2000, §§ 43-44.
[987] *Perry v. the U.K.*, 17 July 2003, § 38.
[988] *Uzun v. Germany*, 2 December 2010, §§ 51-53.
[989] Article 8.2 states that: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national

First, the aim pursued must be one of the legitimate aims listed in article 8.2 of the ECHR (and 52.1 of the CFR). The aim pursued by Unmanned Surveillance is pretty obvious; it is that of crime prevention. However, this aim does not look as legitimate as it first appears. Indeed, the way UASs are being operated is symptomatic of a proactive approach to crime, which has been described by Gonzalez et al., and which we have already outlined in the framework of forensics uses of genetic databases.[990] In short, Gonzalez et al. have identified two different crime-fighting logics at work in police operations: a fundamentally post-crime logic, and a purely preventive logic. Whereas the first tends to collect data in order to facilitate the identification of criminals related to already committed crimes, the second aims processes data not in relation to already existing offences, but in relation to potential future offences. Whereas the legitimacy of the first approach has been acknowledged, that of the second is not as ascertained, as it opens the door to a disproportionate use of data (i.e. threat of the PSP), discrimination, or the reversal of the presumption of innocence.[991]

This is quite obvious in the examples provided by the case study. Accordingly, UAS has noticeably been used for police operations, for example to monitor festivalgoers, especially to monitor individuals acting "suspiciously", or to monitor protests at a right-wing festival and to monitor the Olympic hand-over ceremony at Buckingham Palace. Equally, the Merseyside police force in Liverpool has used two drones to police **"public order" and "prevent anti-social behaviour".** Police in Liverpool have flown the drone over groups of young people loitering in parks.
Furthermore, a "South Coast Partnership" between Kent Police and five other police forces in the UK is seeking **to "introduce drones 'into the routine work of the police, border authorities and other government agencies' across the UK**."
In sum, it is as if constant and global surveillance is to be achieved in order to be proactive, should a crime happen. But is it really legitimate to monitor young people merely walking into parks? Surely the latter is not a crime. If the prevention of crimes is a legitimate aim, one should not turn it into a generalized surveillance or into the detection of undesirable and unaverage behaviour, irrespective of their lawfulness.

As a matter of fact, it can also be argued that these practices are not proportional, or necessary in a democratic society in the meaning of article 8.2 of the ECHR, which entails that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.[992]
Hence, one can wonder whether it is proportionate to monitor a priori innocent individuals in the name of a goal that is defined in terms as broad as "the prevention of anti-social behaviour". Beyond the question of the extent of the monitoring (e.g., scanning a place avery 2 seconds or every 2 hours), it is not improbable that such an approach might end up in reversing the presumption of innocence by turning it into a presumption of guilt. The same goes true concerning the use of such "heavy" measures for behaviours that do not constitute criminal offences and/or minor offences. In addition, is it really necessary in a democratic society? Aren't there less intrusive means that would not lead to a permanent surveillance of all public activities, especially in cases of behaviour, the nature of which is doubtful from a criminal point of view? Consequently, if one agrees that these surveillance measures (which rely upon

---

security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
[990] Gonzalez Fuster et al., 2010, pp. 5-6.
[991] Ibidem.
[992] *Leander v Sweden*, 26 March 1987, §58; Messina v Italy, 2000, §65.

the processing of personal information) might not be necessary in a democratic society; then one has to acknowledge that they may also infringe upon the data quality principle, which requires that the data processed be not excessive to the aim pursued. And in such an hypothesis (that is if the data processed are excessive), is it not the proof that the interference with the right to privacy is disproportionate?

Such proactive surveillance practices put an even heavier burden on citizens' privacy, taking into account that they bear discriminatory consequences. As the case study suggests, "in Western Europe, hardly a marginalised group that is not targeted by UAVs". The Netherlands have used UAVs to "support police in the eviction of a squat", while Belgium, France and Italy have used UASs to monitor "undocumented workers, and undocumented migrants". Therefore, one can argue that a practice that bear such risks is not proportional, and neither necessary in a democratic society.

8.3.2 Data protection perspective

Furthermore, disproportion can also be inferred from a data protection point of view. As a matter of fact, when surveillance is undertaken for objectives that are as broad as "the prevention of anti-social behaviours", one can argue that the Purpose Specification Principle is jeopardised. As mentioned earlier, this principle entails that the processing purpose be specified and specific. Therefore, a goal that is defined in too broad terms may go counter the PSP.

An important parameter to be taken into account is the extent to which UAVs are automated. Indeed, the UAVs described in the case study are automated inasmuch as the pilot controlling them is not on-board but behind a remote control panel. However, one might imagine UAV that could be further automated, as they would not need to be piloted by any human agency, much as is the case with smart CCTVs. In this hypothesis many more data processing operations would be required, since purely automated devices must rely upon a pre-existing database. This entails additional data processing such as the recording, indexation, etc. of the data filmed, as well as the mining of these data for profiling purposes. Moreover, if UASs are to store data, this bears additional data protection consequences, such as the need to enforce the data subjects' subjective rights to access, erasure, etc. In this respect, it is insightful to notice that the Council of Europe has declared that, "the storage of personal data for police purposes should be limited to (…) such data as are necessary to allow police bodies to perform their lawful tasks".[993]

Remaining in a data protection perspective, the Council of Europe is very cautious about the possibility to process personal data for preventive purposes (as has been described above). It states that, "the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence".[994] Moreover, the Council of Europe (CoE) has also warned against the possible "discriminatory drifts" of such practices, as it argues that "the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour (…) should be prohibited".[995]

[993] Council of Europe, Recommendation No. R (87) 15 regulating the use of personal data in the police sector, 1987, Principle 3.1.
[994] Council of Europe, Recommendation No. R (87) 15 regulating the use of personal data in the police sector, 1987, Principle 2.1.
[995] Ibidem, Principle 2.4.

Finally, as far as the obligation to notify the data subject, the CoE distinguishes two possibilities. Either the data have been deleted; either the data subject should be informed where practicable, that information is being held about him as soon as the object of the police activities is no longer likely to be prejudiced.[996]

8.4 BODY SCANNERS

8.4.1 Do they constitute an interference with the right to private life?

Body scanners are scanners that produce an image of the body of a person, which shows whether or not objects are hidden in or under his/her clothes.[997] Because of this characteristic, this data processing device can be described as particularly intrusive, insofar as the privacy of individuals is concerned. Indeed, body scanners can reveal data in the form of images that are strongly entangled with the private life of an individual. For instance, the case study mentions that they can reveal images of naked bodies, which in turns also reveals very sensitive information such as medical information.[998] As evidenced in D.1, the ECtHR considers that the processing of personal data falls within the scope of privacy either because the data are intrinsically linked to the private life, either because the scope of the processing is such that it pertains to it.[999] In this case, it is quite clear that such intimate data are intrinsically linked to the private life of individuals.

Therefore, the question remains as to whether such an interference is lawful or not, according to the three-folded criteria of article 8.2 of the ECHR (legality, legitimate aim, necessity in a democratic society).

As Body scanners are only in a phase test in Europe, it is difficult to assess the legality condition. Instead, we prefer to focus our attention on the conditions of legitimacy, necessity/proportionality.

As far as the legitimacy of the body scanners is concerned, it would seem that the goal pursued is compatible with article 8.2 of the ECHR (i.e., in the interest of national security).

As far as the proportionality and the necessity in a democratic society are concerned, the first thing to take into account is the particularly intrusive nature of body scanners.[1000] As the article 29 WP notices, compared to existing detectors, body scanners reflect by their very name a wider intrusion for the individual.[1001]

Because of this very intrusive nature, it might be argued that they are disproportionate.
The art 29 WP argues that the intrusion capability of a body scanner could reach an acceptable level only if the information provided is strictly limited to the purpose of its implementation: to locate suspected objects without providing images considered to be so intrusive that they raise proportionality issues.[1002]

---

[996] Ibidem, Principle 2.2.
[997] Article 29 Working Party, Consultation, The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, adopted on 11 February 2009, p. 2.
[998] Case study, p. 15.
[999] Gutwirth et al., p. 6.
[1000] Although the level of intrusiveness may vary, see, Article 29 Working Party, Consultation, *loc. cit.*, 2009, p. 8.
[1001] Ibid.
[1002] *Ibid*, p. 8.

The European Commission also proposes a comprehensive set of technical measures that would mitigate the intrusiveness of body scanners.[1003] In addition to that, it is argued that scanners are expected to assist in keeping throughput times at screening point sat an acceptable speed.[1004] But is this sufficient to make these security scanners proportional? In making this assessment, one has to take into consideration that although body scanners are praised for their greater efficiency with respect to classical metal detectors, they are not flawless. As the case study suggests, significant gaps remain in the ability of machines to offer increased security for passengers.[1005] As a matter of fact, Germany has just decided to "postpone a plan to roll out body scanners at airports for security reasons, after a trial phase showed that the devices are incapable of distinguishing armpit sweat from concealed bombs."[1006]
Moreover, body scanners are sometimes presented as an alternative to physical hand-search, which are also considered as intrusive.[1007] However, one has to keep in mind that scanners do not replace body searches. Merely, they precede them, but if a scanner detects something, a search will be unavoidable.[1008]

But beyond the question of whether entirely scanning the body of citizens is proportional, in the sense that it strikes a good balance between its advantages and its costs (i.e., mainly its intrusive nature that highly interferes with our privacy), one needs to determine whether body scanners are necessary in a democratic society, that is, if there aren't less intrusive means that can reach the same goal. Indeed, quoting the European Commission, the EDPS wonders "whether adding new security layers after every incident is an effective means to improve aviation security". In addition to that, the EDPS reminds that it has long outlined the need for a more holistic approach in relation to new measures in the field of law enforcement and fight against terrorism.[1009]
This is corroborated by the article 29 WP that states that, to its knowledge, there has been no evidence presented to show why body scanners are necessary, and why existing measures are not sufficient.[1010]
More evidence is needed in order to make a definitive assessment, but the questions remains nonetheless highly pertinent.
There is therefore a solid risk that body scanners are neither proportional, nor necessary in a democratic society, and hence, that they violate the right to privacy of the citizens of the EU.

8.4.2 Data Protection perspective

As far as data protection legislation is concerned, a crucial point to be determined is whether the data protection directive can be applicable to body scanners. For instance, the European Commission has advocated for the use of Privacy Enhancing Technologies with respect to body scanners. The latter would ensure that, "images analysed by a human reviewer are not linked to the identity of the screened person and are kept 100% anonymous".[1011] This state-

[1003] European Commission, Communication form the Commission to the European Parliament and the Council on the use of Security Scanners at EU airports, COM(2010) 311 final, Brussels, 15 June 2010, pp. 12-13.
[1004] European Commission, 2010, p. 10.
[1005] Case study, p. 14.
[1006] Euobserver, 1 September 2011. http://euobserver.com/22/113479
[1007] See, e.g., European Commission, 2010, p. 11.
[1008] Article 29 Working Party, Consultation, *loc. cit.*, 2009, p. 8.
[1009] EDPS, Comments on the Communication COM (2010) 311 final from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, Brussels, 1 July 2010, p. 1.
[1010] Article 29 Working Party, Consultation, 2009, p. 13.
[1011] European Commission, Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM (2010) 311 final, Brussels 15 June 2010, p. 13.

ment –as laudable as it is, poses big threats to the applicability of the data protection legislative framework. As outlined in the first deliverable, the data protection directive is only applicable to personal data, that is, "any information relating to an identified or identifiable natural person".[1012] In other words, the goal of protecting individuals (through the anonymisation of their data) might actually result with the unintended consequence of depriving them from the protection of the whole data protection framework, since the latter would be inapplicable to non-personal data.

This is highly problematic as it is without doubt that the data collected by body scanners pertain to the privacy of citizens. The case law of the ECtHR is very clear on that: the processing of information pertains to the privacy of individuals either because of the intrinsically private nature of the data processed, either because the scope of the processing is such that it touches upon the privacy.[1013] It is clear in our case that the data at stake are intrinsically private, given that they are so intimate.[1014]
Consequently, we might be confronted in the future to data that are intrinsically private (and thus intrinsically touch upon our privacy), but which are nonetheless anonymous, and hence, out of the scope of the data protection legislative framework. This observation confirms the findings of our first deliverable wherein we emphasised the crucial necessity to make the difference between the rights to privacy and data protection as they have each their own legal significance and role to play.[1015]

But even assuming that data protection legislation applied, some principle would still be jeopardised. The purpose specification principle is again at stake. First, the case study outlines very clearly the risks of secondary uses, such as the storing of data or even its communication on the Internet.[1016]
The data minimisation and data quality principles are also at stake given the highly sensitive nature of the data processed (in the sense of article 8 of the data protection Directive). Body scanners process an incredibly high number of data, the highly sensitive nature of which should have an influence on the assessment of the proportionality of the processing, its relevance, and its adequateness.

As far as the legitimacy of the processing inherently part of body scanning, the article 29 WP is convinced that the appropriate ground is article 7 (f), that is, the processing is necessary for the pursuance of legitimate interests. Accordingly, consent cannot serve as a lawful basis because giving a choice to individual would tend to prove that body scanners are not strictly necessary.[1017] It also adds that the refusal of going through the scanner might create suspicion. Therefore, it can be concluded that this consent is not free in the meaning of the directive (ar-

[1012] Article 2 (a) states that, "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".
[1013] Guwirth et al., 2011, p. 6.
[1014] Although it is true that the definition of personal data is very broad, and has led to extensive definitions (e.g., see opinion 4/2007 on the notion of personal data of the Article 29 Working Party), the point we are trying to make is that conceiving data protection as solely regulating personal data is fundamentally constrained. On the contrary, it should be extended to any processing of information that impacts upon the privacy and/or other fundamental freedoms of citizens. In order to determine which practices to regulate, it is important to correctly articulate data protection to the fundamental right to privacy and to other human rights that function as ~tools.
[1015] Guwirth et al., 2011, pp. 51-52.
[1016] Case study, p. 17.
[1017] Article 29 Working Party, Consultation, *loc. cit.*, 2009, p. 13.

ticle 2). The Working Party goes on to say that the basis for legitimacy should be found in an act of the legislator as body scanners are deployed for public security reasons.[1018]

8.5 RFID: BIOMETRIC PASSPORT AND TRAVEL CARDS

Because RFID passports deal with sensitive personal information (i.e., biometrics), they can be said to interfere with the right to private life, in the meaning of article 8 of the ECHR.[1019] Several points need to be made concerning the proportionality of RFID passports and their necessity in a democratic society.

As far as the proportionality of the device is concerned, the case study outlines several points that lead to think that there is, at least partly, a lack of proportionality.
First, it is important to take into consideration that the RFID passport is a device that presents many security flaws, which, up to this day, have not yet been addressed in an adequate manner. Even more, many observers have acknowledged that the whole process may have been rushed whilst the pace of technical progress was not mature yet. In this respect, the risks bore by e-passport holders is disproportionate in comparison to the advantages the latter may bring. Aiming to achieve a fully automated identification process might also be coined as disproportionate as it entails even more data processing. Also, the doubts raised concerning the efficiency of biometrics for purposes of identification trigger questions on the necessity of purely automated mechanisms.[1020]
The many threats associated to these security flaws raise also the question of the necessity of the device. Indeed, initially the goal of the e-passport was to fight against passport forgery and identity theft. However, the case study argues that e-passport's many security flaws might make passport forgery actually… easier. Such a view is corroborated by the fact that the efficiency of biometry for purposes of identification is far from being obvious. But even more, one has to question the choice for RFID: its contactless nature makes it much more vulnerable than other devices. So why choose this technology to process highly sensitive information, when less vulnerable technology is available? Also, the choice of using RFID poses avoidable threats on locational privacy, that is, the possibility of determining the location of an individual through the monitoring of the RFID tag (no matter whether the RFID tag actually contains personal information, or solely an identification number).[1021]

In a nutshell, because of its many flaws and risks for privacy –stemming both from the use of biometric and RFID technology, the e-passport appears as disproportionate with respect to its goal. Moreover, these very flaws impact negatively on its efficiency, and it can be argued that other kinds of passports (such as paper versions) might actually work better. One can therefore wonder whether this device is necessary in a democratic society.

From a data protection point of view, the many security and technical flaws appear as inconsistent with article 17 of the data protection Directive, which requires that information-processing devices be secure.[1022]

[1018] Article 29 Working Party, Opinion 15/2001 on the definition of consent, WP 187, Adopted on 13 July 2011, p. 15.
[1019] See for instance Council of Europe, Report on the application of the principles of Convention 108 to the collection and processing of biometric data, 2005, chapter I.
[1020] Case study, p. 16
[1021] Case study, p. 17.
[1022] Article 17 states that: "1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or acciden-

Also, one might question the rationale of using two biometric identifiers with respect to the data quality principle. Furthermore, in situations where RFID chips only store a serial number, the recourse to biometric databases will be inevitable and will raise questions in terms of data minimisation.[1023]
A consistent application of the Purpose Specification Principle should also cast doubt on fully automated passport verifications, as human agency would avoid additional data processing.

As far as RFID travel cards are concerned, once more, the fact that so many security threats exist puts into question the proportionality of the device from a privacy viewpoint, and raise concerns as far as article 17 of the data protection directive is concerned. Another important threat with respect to privacy is that of locational privacy, i.e., the possibility to track individuals' public transportation patterns. Consequently, the question here is whether this important threat to privacy is proportionate or not, and hence, if there are some possibilities to mitigate it. The case study mentions that in some countries such as the U.K., data stored in relation to the London Oyster Card is available online to anyone with the card's serial number. In this case, it is quite easy, not only to access the data, but also to track the user. This could be qualified as disproportionate. Therefore, access to personal data should be more difficult, or, the latter could be anonymised. However, in this case (just like with body scanners), the applicability of the data protection framework would be put into question.[1024]
Also, the fact much personal information is stored either on the card either on the back-end system, raises concerns as far as the purpose specification and data quality principles are concerned: is it strictly necessary to store so much personal information, especially taking into account the fact that it is (too) easily accessible in some countries? Plus, once the information is stored in a database, there are many possibilities for unlawful secondary uses.

8.6 SECOND-GENERATION BIOMETRICS: BEHAVIOURAL AND SOFT BIOMETRICS AND HUMAN ENHANCEMENT TECHNOLOGIES

8.6.1 Second-generation biometrics

The characteristics of second-generation biometrics raise concerns in terms of privacy and of data protection. Beyond traditional biometric issues such as that of databases, or the different types of possible biometric authentication, the inherent characteristics of second-generation biometrics raise concerns in their own rights. Indeed, whereas first generation biometrics relies upon static characteristics in order to identify individuals, second-generation biometrics collect dynamic or behavioural characteristics.

First, there are some costs to new biometrics. Indeed, as the case study suggests, behavioural biometrics do not enable the identification capabilities of first generation biometrics. For in-

---

tal loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. (…)"

[1023] See, Council of Europe, Report on the application of the principles of Convention 108 to the collection and processing of biometric data, 2005, especially chapter III on the architecture of the system, and chapter IV on the application of data protection principles.

[1024] As a matter of fact, the Article 29 WP considers RFID tags as personal information as long as they lead to personal information in the back-end system. Were they to lead to anonymised information, its opinion might be different. See, Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data 4/2007, 01248/07/EN, WP 136, Adopted on 20th June 2007.

stance, signature dynamics recognition will be outperformed by fingerprint analysis. Because of this weakness in the identification process, it would seem necessary for second-generation biometrics to resort to multimodal systems of identification, thereby contradicting the data minimisation principle.
This is also the case for so-called soft-biometrics that can determine the gender, or ethnicity of a person, but which lack the distinctiveness and permanence of first generation biometrics in order to single out a particular individual. One can therefore wonder on the added value and hence, necessity of resorting to this type of identification technology that processes increasingly sensitive information.
Furthermore, along with second-generation biometrics, comes the possibility of identification from distance, with no cooperation or action required from the data subject. This poses some threats in terms of the data subjects right to be informed of a data processing.

All in all, the development of second-generation biometrics is intriguing. If one keeps in mind the fact that biometrics can be defined as "the automated recognition of an individual's identity", and that second generation biometrics precisely fail to do so in a manner that is as consistent as that of first generation biometrics, one can therefore wonder about their necessity. But their proportionality is also at stake. Indeed, behavioural or soft biometrics are considered to be much more intimate and may sometimes qualify as sensitive in the meaning of article 8 of the Data Protection Directive. This is especially true in the light of multimodal identification, and distant identification. The fact that an individual passing can be identified without his knowledge and through the use of particularly sensitive data appears to be problematic. Moreover, such a permanent and uninterrupted surveillance is not void of discrimination problems.

8.6.2 Human enhancement technologies

The two human enhancement technologies touched upon by the case study are Brain Computer Interface (BCI) and neuro-enhancement.

BCI technology consists in the recording of electrical activities of the brain. Therefore, it can be said that it goes a step further than technologies processing genetic data, as the brain's electrical impulses enable a third party to directly scrutinize the data subject's mind and way of thinking. Their degree of sensitivity is thus maybe higher than that of genetic data. BCI appears as a step further into penetrating the intimacy of individuals.

Yet, this processing of personal data is not *ipso facto* contrary to the privacy of individuals.

As a matter of fact, it appears from the case study that one of the main goals of BCI is to enable partially or fully partially paralysed people to communicate and regain at least a bit of control over their lives. In other words, BCI can be seen as a way to empower people, and in that sense it reflects the emancipatory nature of privacy.
As we have evidenced in the first deliverable, the ECtHR case law has gone on to conceptualise privacy as a relational concept that goes well beyond a mere right to intimacy, ultimately leading to the important consequence that "'private life' is a broad term encompassing, *inter alia*, aspects of an individual's physical and social identity including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world".[1025] This right to self-determination includes, *inter alia*, the

[1025] Evans vs United Kingdom, 10 April 2007, § 71.

right to gender identification, or the right to sexual orientation.[1026] In this respect, it is interesting to observe that the ECtHR has also declared that participating to S&M practices as the "victim" was encompassed within the scope of article 8, provided the consent and the will of the "victim" are respected.[1027] Therefore, in this respect, the fact for patients to willingly resort to BCI interfaces seems compatible with their right to privacy, even though it might result with the discovering of some of their most intimate information.[1028] As a matter of fact, these developments are equally valid with respect to neuro-enhancement. However, the case study emphasises well that the risks of abuses are well present, and were that to be the case, the right to privacy would be infringed upon.

Yet, even in the hypothesis wherein BCI given the highly sensitive nature of the data at stake, it is important to process in a proportionate manner. This might mean that the respect for privacy entails that it is not possible to store this kind of information (cf. *supra* whole genomic sequencing), or that some special safeguards must be taken in order to avoid abuses of power, or even that not all uses are lawful.

From a data protection point of view, the fact that the data processed are so sensitive probably entails that the lawfulness of commercial use is quite dubious (cf. art. 8 of the data protection Directive). Furthermore, it is important to re-emphasise that from a data protection perspective, consent alone is not a sufficient basis to declare a data processing legitimate.[1029] Therefore, and given the extremely sensitive nature of the data, it is likely that BCI will only be allowed for medical purposes (but probably not commercial uses).

8.7 CONCLUSIONS

Two sets of conclusions can be drawn from the case studies analysed.

The first one concerns the relationship between the legal rights to privacy and data protection. In the first deliverable we had emphasised the fact the privacy and data protection are two different legal instruments with a different content. Our analysis proves that this distinction is not merely theoretical.
The body scanners case (and to some extent the RFID one) shows that the scope of the two rights is not identical, since non-personal data would still interfere with the right to privacy of individuals.
But even when the two rights are applicable, the scope of their protection doesn't necessarily equate. As far as the processing of personal information is concerned, both right require that this processing be proportionate (either according to the data minimisation principle, either according the article 8.2 and the "necessity in a democratic society" condition). Yet, the meaning of this proportionality can be different. This was clear in the genomic sequencing case study, where we evidenced that some processing (e.g., genetic biobanks) might be proportionate from a data protection perspective, but not from a privacy perspective. In order to

[1026] See e.g. the B. v. France, 25 March 1992, Series A no. 232-C, § 63; Burghartz v. Switzerland, 22 February 1994, Series A no. 280-B, § 24; Dudgeon v. the United Kingdom, 22 October 1991, Series A no. 45, § 41; Laskey, Jaggard and Brown v. the United Kingdom, 19 February 1997, Reports 1997-1, § 36.
[1027] *K.A. and A.D. v. Belgium*, 17 February 2005, § 85. On this case, see also, Gutwirth, S., De Hert, P., De seks is hard maar seks (dura sex sed sex). Het arrest K.A. en A.D. tegen België, *Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, from Panopticon, vol.26, n. 3, 2005, pp. 1-14.
[1028] That is not to say that BCI, or neuro-enhancement, are totally void of threats for the privacy of individuals. In this respect, see section 1.2.4 of chapter 7. The point however, is that the role of consent will differ greatly depending upon whether we adopt a privacy or data protection perspective.
[1029] Cf. *Supra*, genomic sequencing.

understand this discrepancy, one must keep in mind that the "data protection proportionality" is always assessed in reference to the aim pursued, whereas the "privacy proportionality" puts the question in the bigger framework of the democratic society. Ultimately, this can be linked back to their different nature, data protection being a *transparency* tool, and privacy being an *opacity* tool.[1030] Whereas the former focuses on each processing separately and aims at making sure that they are undertaken according to pre-existing criteria, the latter aims at protecting the autonomy and self-determination of each individual, which requires going beyond the mere verification of the respect of the data processing criteria.
The situation is not however one-sided. In the human enhancement case study we have had the opportunity to emphasise the emancipatory (and non-paternalistic) nature of the right to privacy. Because self-determination of the individual is at the heart of this right, what he/she consents to do is important. This contrasts sharply with the right to data protection, where it is crucial to understand that consent alone does not constitute a legitimate for the processing of personal information.

The second conclusion stems from the observation of a trend that is at work within all the case-studies.

First, they can be qualified as intrusive since they all process sensitive data. Most of these technologies deal with genetic, biometric, or even brain data. In this respect, there seems to be a trend to use always more and more intimate data of citizens. The classical identifiers such as the name seem out-dated.

Second, the extent of the processing is very important: instead of trying to minimize the processing of personal data, these technologies seem instead to nurture a maximal processing of data. As if the data minimisation principle was turned into a "data maximisation principle". If such a stance can sometimes be justified in the case of medical research, this is hardly the case for police operations. Furthermore, the extent of the processing concerns not only the amount of data collected, but also the different types of operations undertaken. One of the biggest threats lies in the storing of data that ought not to be: once the data are stored, practically the door is open to a multiplicity of secondary uses, thereby violating the PSP. And what about risks stemming from security failures?
When thinking about the possible roots and reasons of this "data maximisation" phenomenon, one possible cause might be the trend towards more and more automation of processes. Indeed, the automatic interlinking between genomic databases, but also the automated verification of passports, unmanned surveillance, or body scanners, all rely to some extent upon the automatic processing of data. One has to wonder why such a trend is at work. Would there be a belief that the more an operation is automated, and the more data it processes, the better results it will achieve, and most importantly, it will put an end to the necessary cracks and failures that are inherently contingent to any human agency?
However, with respect to CCTVs, many studies in the field of surveillance have shown evidence that a huge number of cameras, interlinked between each other and with other databases, didn't equate to a zero risk situation.[1031] Moreover, it evidenced other shortcomings such as high rates of false positives. This situation echoes –among others, the position of the EDPS, which argues that data protection principles do not constitute mere obstacles to a fully satisfying data processing operations, but that, on the contrary, they constitute the very condi-

[1030] On the difference between privacy as an opacity tool and data protection as a transparency tool, see Gutwirth et al., 2011, pp. 7-8.
[1031] Among many, see Goold, B. CCTV and policing: public area surveillance and police practices in Britain, Oxford: Oxford University Press, 2004.

tions for a data processing to be successful. The EDPS outlines the data quality principle that requires indeed having accurate data, or that unnecessary information should be eliminated rather than encumbering databases.[1032] In other words, respecting the purpose specification principle might actually help achieving better results. These remarks have to be contrasted with our observations according to which the PSP seems to be particularly shaken by extensive definitions of the processing purposes that may end up emptying the principle of its substance, which end up in disproportionate and/or discriminatory processing.

Therefore, not only this "data maximisation" stance threatens the efficiency of data processing activities, but it also presents some risks in terms of data protection, as one could argue that it goes counter the very rationale that is at the heart of data protection legislation, that is, the processing of personal data should be avoided as much as possible since it carries inherent risks stemming from the lack of control individuals have over their personal information once they are being processed by a third party.[1033] There is an awareness in data protection legislation that once the informational materialisation of individuals (i.e., their personal information) is in the hand of third parties, there exists risks of abuses. A typical abuse is the violation of individuals' right to privacy, but with the processing of ever more sensitive data, discrimination is also acquiring more importance.
Consequently, any system processing personal information should respect this core logic of data protection legislation, and should be operated in a manner less likely to produce risks and abuses, even though it might entail abandoning some of the myths that have come along with the modern notion of progress.

8.8 REFERENCES

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data 4/2007, 01248/07/EN, WP 136, Adopted on 20th June 2007.

Article 29 Data Protection Working Party, Working Document on Genetic Data, 12178/03/EN, WP 91, Adopted on 17 March 2004.

Article 29 Working Party, Consultation, The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, adopted on 11 February 2009.

Article 29 Working Party, Working Document on data protection issues related to RFID technology, 10107/05/EN, WP 105, Adopted on 19 January 2005, p. 9. This expression might be misleading insofar as it would suggest that data should be conserved. On the opposite, data should be conserved as little as possible.

Council of Europe, Recommendation No. 4 (83) 10 on the protection of personal data used for scientific research and statistics, 23 Septembre 1983.

Council of Europe, Recommendation No. R (87) 15 regulating the use of personal data in the police sector, 1987.

Council of Europe, Report on the application of the principles of Convention 108 to the collection and processing of biometric data, 2005.

De Hert, Paul, and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwagne,

[1032] EDPS, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union', 2011/C 181/01, 22 June 2011, article 22.
[1033] Hence the list of subjective rights, in order to mitigate this loss of control.

Sjaak Nouwt (eds.), Reinventing Data Protection? , Doordrecht: Springer, 2009, pp. 20-23.
EDPS, Comments on the Communication COM (2010) 311 final from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, Brussels 1 July 2010.
EDPS, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union', 2011/C 181/01, 22 June 2011.
Els, Kindt, and Müller, Lorenz, "D13.4: The privacy legal framework for biometrics", FIDIS - Future of Identity in the Information Society, 2009, p. 17. Available on the following website,
http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis_deliverable13_4_v_1.1.pdf;
Euobserver, 1 September 2011. http://euobserver.com/22/113479
European Commission, Communication form the Commission to the European Parliament and the Council on the use of Security Scanners at EU airports, COM(2010) 311 final, Brussels, 15 June 2010, pp. 12-13.
Gonzalez Fuster Gloria, Paul De Hert, Erika Eva Ellyne, Serge Gutwirth, "Huber, Marper and Others: Throwing new light on the shadows of suspicion", INEX Policy Brief, No. 11, Centre for European Policy Studies (CEPS), 2010, pp. 2-3.
Goold, B. CCTV and policing: public area surveillance and police practices in Britain, Oxford: Oxford University Press, 2004.
Gutwirth, Serge, Privacy and the Information Age, Rowman & Littlefield, Lanham, 2002.
Gutwirth, Serge, Raphael Gellert, Rocco Bellanova, Michael Friedewald, Philip Schütz, David Wright, Emilio Mordini, and Silvia Venier, Deliverable D.1: Legal, social, economic and ethical conceptualisations of privacy and data protection, PRESCIENT: Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment, 2011.

Case law of the European Court of Human Rights

- Amann v. Switzerland, 16 February 2000.
- Association for European Integration and Human Rights and Ekimdzhev vs. Bulgaria, 30 January 2008.
- Halford v. the United Kingdom, 25 June 1997.
- Klass and Others v. Germany, 6 September 1978
- Malone v. the U.K., 26 April 1985.
- Niemietz v. Germany, 16 December 1992.
- P.G. and J.H. v. the U.K., 25 September 2001.
- Peck v. the U.K., 28 January 2003.
- Perry v. the U.K., 17 July 2003.
- Rotaru v. Romania, 4 May 2000.
- S. and Marprer v. The United Kingdom, 4 December 2008.
- Uzun v. Germany, 2 December 2010.
- Weber and Saravia v. Germany, 2006.

Chapter 9, Synthesising privacy and data protection considerations

Rachel Finn and David Wright
Trilateral Research & Consulting, LLP

9.1 INTRODUCTION

This chapter organises and distils the detailed information presented in the case studies and the legal chapter to consider what privacy, data protection, ethical and social impacts are pertinent in relation to the five case studies, whether the existing legal framework adequately address these potential impacts and, if not, what policy interventions might address these impacts. The chapter begins with a review of the impacts associated with each of the case study technologies. In the second section, we use the different aspects of privacy outlined in the first PRESICENT deliverable to consider how new and emerging technologies are mapped against these different aspects of privacy. These different facets of privacy are then considered in relation to the legal uncertainties chapter, where we argue for a flexible, continuous consideration of privacy and data protection when developing and deploying new technologies. The next section of the chapter examines the ethical and social impacts of the case studies by considering their impact upon human dignity, equality and the rule of law. The chapter concludes with brief policy recommendations that will be further developed through subsequent work packages and tasks throughout the project.

9.2 PRIVACY, DATA PROTECTION AND ETHICAL ISSUES IN CASE STUDIES

9.2.1 RFID

This report undertakes two case studies in relation to RFID-enabled travel documents in Europe. The first focuses on RFID-enabled travel cards such as, Oyster Cards in London, which integrate RFID technology with the use of mass transportation in urban areas. The second focuses on RFID-enabled passports, also called e-passports that are currently being introduced in most countries. Both case studies focused on RFID-enabled travel documents identified privacy, data protection and ethical and social issues in the deployment of these technologies.

Privacy concerns

Privacy issues associated with RFID travel documents included the possibility of clandestine tracking, unauthorised reading, cloning, hotlisting[1034] and unauthorised marketing. A key potentially privacy-infringing practice is the tracking of individuals using information from the communication between a travel card and a reader or using the RFID signal in their e-passports. Specifically, the RFID-enabled travel card infrastructure enables tracking, by virtue of the fact that individuals' last known locations or their movements as they use public transport can be gleaned from travel card data. Retrospective tracking is possible if location, time and other information stored on databases is combined. This information has been used by police to check suspects' whereabouts or movements during criminal investigations.[1035] However, Langheinrich points out that the association between the individual and the tag can be spurious (e.g., if the card is stolen or given to another person), and the association between an individual and a tag is difficult to break once it is made. This generalised threat materialises into specific threats. Information about passengers' latest entry and exit stations from Japanese public transport systems are stored on the Suica card and can be read by basic, commer-

[1034] Hotlisting consists of compiling all the available information concerning an individual, so that when an identifier is detected it can be linked to all the other information available concerning this particular individual.
[1035] *The Guardian*, "Oyster data use rises in crime clampdown", 13 Mar 2006. http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation and Octopus Holdings Limited, "Customer Data Protection", 2009.

cially available RFID readers, which could facilitate stalking.[1036] British newspapers have also found that the data stored in relation to the London Oyster card is available online to "anyone with the card's serial number", or who takes the card to a payment station.[1037] Such data has been used in divorce proceedings as evidence of infidelity. However, in most places, police or other authorities must provide a search warrant or court order in order to be given access to the data.[1038] Tracking is also possible in relation to e-passports. Because the passive RFID chips in e-passports are standardised (cf. ISO 14443), passports' tags will broadcast the RFID chip's unique identifier upon initiation coming from any reader, since this operation does not require authentication. Clandestine tracking is thereby made possible by reading this unique identifier, storing it and following its signal.

Threats around the unauthorised reading of RFID-enabled documents were primarily associated with RFID-enabled passports. The case study identifies a number of security mechanisms intended to reduce this threat; however even with these security mechanisms, some threat remains. Unauthorised reading may take place in public space, can occur without the passport holder's knowledge, and can violate data protection principles in that it can be used to reveal an individual's personal details, biometric information or their citizenship. In RFID-enabled passports, basic access codes and Faraday cages[1039] are built into the passport and used to prevent unauthorised reading. Unfortunately, gaps have been discovered in these protection mechanisms. IBM researchers have determined that basic access codes could enable counterfeiting as it is possible for a forger to splice together a valid electronic signature with false identity information and biometric components.[1040] Furthermore, although they constitute an effective method for reducing the opportunity for unauthorised reading of the passport, Faraday cages do not prevent eavesdropping on legitimate conversations between readers and tags. In addition to gaps in the effectiveness of these measures, the relevance of these measures over time needs to be addressed. For example, the case study finds that some stakeholders have already voiced concern over the fact the cryptographic measures do not possess the desired long-term security needed for e-passport applications (their validity is estimated to a maximum of 10 years).[1041]

Other privacy threats related to RFID travel documents include cloning, hotlisting and unauthorised marketing. An identical clone of an RFID chip containing travel card or passport information can be used in place of an original without the original user's knowledge. Scientists have demonstrated that both travel cards and e-passports can be cloned, and have used them to ride the London underground free for a day[1042] and create new passport chips[1043].

[1036] Organisation for Economic Co-operation and Development, "RFID Guidance and Reports", *OECD Digital Economy Papers*, No. 152, OECD publishing, 2008, p. 42.

[1037] Bloomfield, Steve, "How an Oyster Card can Ruin your Marriage", *The Independent on Sunday*, 19 Feb 2006. http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html

[1038] Octopus Holdings Limited, "Customer Data Protection", 2009.

[1039] Faraday cages are a metallic shielding embedded in the passport cover and designed to protect it from electronic eavesdropping.

[1040] Kc, Guarav S., and Paul A. Karger, *IBM Research Report: Preventing Attacks on Machine Readable Travel Documents (MRTDs)*, IBM Research Division, Yorktown Heights, NY, 10 March 2006, p. 6, cited in Bronk, Christopher, "Innovation By Policy: A Study of the Electronic Passport", *Social Science Research Network*, May 2007, p. 31. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1557728

[1041] Buchmann, J., A. May and U. Vollmer, "Perspectives for Cryptographic Long-Term Security", *Communications of the ACM*, Vol. 49, No 9, September 2006, p. 54.

[1042] Miller, Vikki, "Oyster card: fears over Mifare security", *The Telegraph*, 21 June 2008. http://www.telegraph.co.uk/news/newstopics/politics/2168791/Oyster-card-fears-over-Mifare-security.html

Hotlisting consists of compiling all the available information concerning an individual, so that when an identifier is detected it can be linked to all the other information available concerning this particular individual.[1044] In this way, authorities could be informed that a travel document connected to a particular individual, or an individual with particular characteristics, has been read in a particular place at a particular time. The unauthorised use of personal information also represents a privacy threat. Marketing staff could target the individual based on the personal data he or she is required to submit in an application form for a travel card. Companies could aggregate these pieces of information to construct sophisticated consumer profiles.[1045] This is especially true if contactless travel cards are expanded for use as payment for other small items. Van't Hof and Cornelissen found that the Dutch Railways have been "open" about their intention to use data from the OV-chipkaarts for marketing purposes, although the railway company does not specify what type of marketing.[1046]

Data protection issues

The relative (in)security of personal information on databases represents a threat to personal data protection. RFID systems are composed of tags, readers and back-end databases where the unique identifier on the RFID chip is linked with personal information. In some cases, the personal information stored on an RFID chip can be read directly from the tag through unauthorised reading. However, systems that store personal data, for example biometric data, in back-end databases may also be vulnerable to security threats such as hacking, unauthorised access or unauthorised disclosure. This data protection threat was demonstrated by a Dutch travel card researcher finding that her phone number and address was accessible to bus drivers as well as other individuals associated with the public transport system. Some systems have attempted to protect individuals from this threat by separating personal information from the RFID chip in the e-passport. Some e-passports' RFID chips do not store any personal information except a code or serial number, which is then used by the reader to call up the relevant information stored in a database.[1047] While this helps to prevent data breaches as a result of unauthorised reading, this solution requires vast amounts of highly sensitive personal information, such as biometrics, to be stored in a unique database. In consequence, some authors have recommended that e-passports store biometric data, one of the rare cases where personal information should be stored on-tag.[1048]

Ethical and social issues

The consequences of these privacy and data protection threats present ethical and social issues. Such issues include the potential for power differentials between those operating RFID

[1043] Juels, Ari, David Molnar and David Wagner, "Security and Privacy Issues in E-passports", in *Security and Privacy for Emerging Areas in Communications Networks,* IEEE Computer Society, Washington, DC, 2005.
[1044] Juels et al., 2005, p. 79.
[1045] Srivastava, Lara, "Radio frequency identification: ubiquity for humanity", *info*, Vol. 9, No. 1, 2007, pp. 4-14.
[1046] van't Hof, Christian, and Jessica Cornelissen, *RFID and Identity Management in Everyday Life*, Deliverable No.2 of the project "RFID & Identity Management" commissioned by STOA and carried out by ETAG, October 2006 http://www.itas.fzk.de/eng/etag/document/hoco06a.pdf
[1047] van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij and Claudio Borean, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, Office for Official Publications of the European Communities, Luxembourg, 2007, p. 197.
[1048] Henrici, Dirk, *RFID Security and Privacy – Concepts, Protocols, and Architectures*, Springer, Berlin, 2008, p. 21; see also Hornung, G., *The European regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, 2007, p. 4. http://www.law.ed.ac.uk/ahrc/scripted/vol4-3/hornung.asp

travel document systems and individuals who carry the documents, and the potential for denial of services surrounding the unauthorised use of their personal information. The e-passport case study argued that such a power imbalance carries a possibility of continuous observation and collection of data from individuals, which may impact human dignity. The consequences of these processes could be a centralisation and aggregation of information about individuals.[1049] Furthermore, this data aggregation could be occurring without people's knowledge.

A second aspect of this potential for power imbalance is that data processers can categorise individuals and/or discriminate against them based on the information collected about them, thereby impacting on a principle of equality. In direct marketing scenarios, this could mean that individuals are offered products based on their generic "profile". Individuals might also experience categorisation and discrimination as a result of the unauthorised use of their personal data. Often travel documents contain enough information to commit identity theft, which could result in denial of a job, a mortgage or some other social privilege. Clearly, the mitigation of such threats and their consequences requires robust, multidimensional impact assessments, one purpose of which is to identify privacy and ethical risks and solutions to overcome these risks.

9.2.2 New surveillance technologies

This case study identifies the privacy, data protection, ethical and social concerns surrounding the use of new surveillance technologies in Europe, and focuses on two technologies, whole body imaging scanners and unmanned aircraft systems (UASs), both of which have newly emerging civil applications. The current development and deployment of these technologies in civil applications have raised ethical, privacy and data protection issues.

Body imaging scanners

Hundreds of whole body imaging scanners are currently deployed in airports in the USA, Europe, Canada, Nigeria and Russia. Other countries are conducting trials or considering their use. Significantly, this deployment of whole body scanners has raised controversy around the world in relation to privacy, data protection, ethical and social issues.

Privacy concerns raised by body scanners have mainly centred on two key issues, the revealing of individuals' naked bodies and revealing information about medical conditions. In terms of revealing naked bodies, privacy advocates argue that this loss of privacy is disproportionate to any gains in security. Academics, privacy advocates, politicians and journalists have all warned that the images resulting from the different types of body scanners currently deployed in airports and other contexts reveal an individual's "naked body", including "the form, shape and size of genitals, buttocks and female breasts".[1050] The issue of "naked images" has also raised questions surrounding child protection laws, and EPIC has argued that the capacity for viewing, storage and recall of images of children may contravene child protection laws.[1051] According to privacy advocates, the images also show details of medical conditions that may

[1049] Spiekermann, Sarah, *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*, Shaker Verlag, Aachen, 2008, p. 67.
[1050] Klitou, Demetrius, "Backscatter body scanners – A strip search by other means", *Computer Law & Security Report*, Vol. 24, Issue 4, 2008, pp. 316-325 [p. 317].
[1051] Electronic Privacy Information Center (EPIC), "Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding", June 2005. http://epic.org/privacy/surveillance/spotlight/0605/

be embarrassing for individuals. In 2002, the ACLU asserted that "passengers expect privacy underneath their clothing and should not be required to display highly personal details of their bodies such as evidence of mastectomies, colostomy appliances, penile implants, catheter tubes and the size of their breasts or genitals as a pre-requisite to boarding a plane".[1052] Despite these concerns, authorities, such as the UK Department for Transport, have argued that any loss of body privacy is proportionate and legitimate in relation to the security concerns that body scanners address.[1053]

Data protection concerns revolve around protection of personal data that the scanners generate, including the storage and transmission of images. According to the US Transportation Safety Administration (TSA) the scanners used in US airports do not store, print or transmit images.[1054] However, a Freedom of Information Act request by EPIC to the TSA found that machines come with the capability to store and transmit images, but this is disabled when they are deployed to airports.[1055] EPIC argues that the fact that this capability could be re-enabled represents a data protection risk to passengers.[1056] EPIC further notes that the TSA does not have a stellar reputation for protecting passenger data.[1057] Privacy International is also concerned that some employees operating scanners will experience an "irresistible pull" to store or transmit images if a "celebrity or someone with an unusual... body goes through the system".[1058] In fact, images from body imaging scanners have been posted on the Internet in a breach of the fundamental rights of thousands of people in the USA.[1059]

The effects of the use of body scanners on air travellers lead to ethical and social concerns related to other fundamental rights, including human dignity, freedom from discrimination and the right to travel. According to Privacy International, the use of body scanners amounts to a significant – and for some people humiliating – assault on the essential dignity of passengers that citizens in a free nation should not have to tolerate.[1060] The group also cautions that "intrusive technologies" are often introduced with a range of safeguards, but once the technology gains public acceptance, these safeguards are gradually stripped away.[1061] The revealing of "naked" images has prevented some groups and individuals, such as Muslim women

[1052] American Civil Liberties Union, "The ACLU's view on body scanners", 15 Mar 2002. http://www.aclu.org/technology-and-liberty/body-scanners

[1053] Department for Transport, *Impact Assessment on the use of security scanners at UK airports*, 29 Mar 2001. http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/consultations/open/2010-23/

[1054] Heussner, Ki Mae, "Air Security: Could Technology Have Stopped Christmas Attack?", *ABC News*, 29 Dec. 2009. http://abcnews.go.com/Technology/AheadoftheCurve/air-security-technology-stopped-xmas-attack/story?id=9436877

[1055] Zetter, Kim, "Airport Scanners Can Store, Transmit Images", *Wired News*, 11 January 2010. http://www.wired.com/threatlevel/2010/01/airport-scanners/

[1056] Rucker, Philip, "US airports say seeing is believing as passengers face body-scan drill", *Sydney Morning Herald*, 5 Jan 2010. http://www.smh.com.au/travel/travel-news/us-airports-say-seeing-is-believing-as-passengers-face-bodyscan-drill-20100104-lq6o.html

[1057] EPIC, "Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding", 2005.

[1058] Privacy International, "PI statement on proposed deployments of body scanners in airports", 31 Dec 2009. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-

[1059] European Economic and Social Committee, Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM(2010) 311 final, Brussels, 16 Feb 2011, p. 4.

[1060] Privacy International, op. cit., 2009.

[1061] ACLU, "Backgrounder on Body Scanners and 'Virtual Strip Searches'", 8 Jan 2010. http://www.aclu.org/technology-and-liberty/aclu-backgrounder-body-scanners-and-virtual-strip-searches

and religious Jewish women[1062], as well as any others "whose religious beliefs include a perspective on bodily modesty"[1063], from exercising their right to travel. This is because in some countries, such as the UK where no alternative is offered, individuals forfeit their right to fly if they refuse to undergo a body scan.[1064] Thus, the use of body scanners impacts upon the principle of the rule of law including religious freedom and freedom to travel outside one's own country.

Unmanned aircraft systems

In contrast to airport body scanners, the use of unmanned aircraft systems (UASs) has generated significantly less debate around privacy and data protection. This has occurred despite a slow increase in the introduction of UASs in civil applications, such as law enforcement, border patrol and other regulatory surveillance. Privacy is notable by its absence in many discussions about UAS devices, which may be partly explained by their current similarity to existing forms of surveillance such as CCTV surveillance or surveillance by police helicopter.

Despite this relative silence, some journalists, in particular, have discussed the potential privacy impacts associated with an expansion of UAS surveillance to civil society. A report in *The Economist* notes that UAVs are cheaper than satellites and fixed cameras and that they can "peek more easily", because they can hover silently and may soon be able to fly inside buildings.[1065] *The Economist* also quotes an FAA spokesman who stated that "it smacks of Big Brother if every time you look up there's a bug looking at you".[1066] In *The Guardian*, a Professor of Robotics at Sheffield University stated that it was necessary to have a public consultation about the use of UASs.[1067] According to EPIC, UAVs represent "a new capability" for the US federal government "to monitor citizens clandestinely".[1068] Other journalists note that they are an extension of "Big Brother Britain"[1069] and "quite intrusive"[1070]. Journalists also note that specific victims of the mass deployment of UASs in civil air space could be celebrities who are subject to paparazzi drones.

This potential for negative impacts on privacy is particularly significant since UAS surveillance is much more covert than CCTV or helicopter surveillance to which it has been compared. Specifically, the lack of noise and relative invisibility of UASs mean that individuals

---

[1062] Quinn, Ben, "Why Europe doesn't want an invasion of body scanners", *Christian Science Monitor*, 26 Jan 2010. http://www.csmonitor.com/World/Europe/2010/0126/Why-Europe-doesn-t-want-an-invasion-of-body-scanners

[1063] *CBC News*, "Airport scanners invade privacy: advocate", 5 Jan 2010. http://www.cbc.ca/canada/british-columbia/story/2010/01/05/bc-airport-scanners-civil-liberties-vonn.html

[1064] Mason, Wyatt, "Scanners Gone Wild", *The New York Times*, 3 Dec 2010. http://www.nytimes.com/2010/12/05/magazine/05FOB-wwln-t.html?ref=technology

[1065] *The Economist*, "Unmanned aircraft: The fly's a spy", 1 Nov 2007. http://www.economist.com/displaystory.cfm?story_id=10059596

[1066] Ibid.

[1067] Randerson, James, "Eye in the sky: police use drone to spy on V festival", *The Guardian*, 21 Aug 2007. http://www.guardian.co.uk/uk/2007/aug/21/ukcrime.musicnews

[1068] Electronic Privacy Information Center, *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking*, Spotlight on Surveillance, August 2005. http://epic.org/privacy/surveillance/spotlight/0805/

[1069] Hull, Liz, "Drone makes first UK 'arrest' as police catch car thief hiding under bushes", *Daily Mail*, 12 Feb 2010. http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html#ixzz1JV7EKR1N

[1070] Sia, Richard H.P., "Agencies see homeland security role for surveillance drones", *CongressDaily*, 12 Dec 2002. http://www.govexec.com/dailyfed/1202/121202sia.htm

do not know if they are being monitored. For example, McBride notes that conventional surveillance aircraft, such as helicopters, provide auditory notice that they are approaching and allow a person "to take measures to keep private those activities that they do not wish to expose to public view".[1071] This could introduce anticipatory conformity (a "chilling effect") where individuals alter their behaviour because they believe they may be under surveillance at all times.[1072]

UAS devices have also prompted ethical and social concerns regarding the distance between UAS operators and their actions on the ground, which could impact upon human dignity. UASs have been blamed for significant losses of life on the ground in combat zones, and the removal of soldiers "from the human consequences of their actions"[1073], which, according to Hayes of Big Brother Watch, may add to a Playstation mentality.[1074] Furthermore, drones view everyone as a suspect because "everyone" visible to the drone is "monitored, photographed, tracked and targeted".[1075] While some law enforcement stakeholders view UASs as a technologically neutral tool at their disposal, Nevins warns that these stakeholders may take advantage of these new tools with significant potential for mission creep.[1076] This could potentially result in a restriction on freedom[1077], and negative implications for civil rights[1078]. These ethical concerns become intertwined with safety and human dignity concerns in relation to the potential for UASs to carry weapons, including non-lethal weapons.

9.2.3 Second-generation biometrics

In parallel with their wider deployment, biometrics have the potential to raise critical privacy, data protection, ethical and social concerns, and these non-technical factors deeply impact the acceptability of biometric identification methods. Most general concerns raised by biometrics are related to the protection of individual values, such as privacy, autonomy, body integrity, dignity and personal liberty. However, the second-generation biometrics case study argues that the most critical implications of next-generation biometrics are that future biometric recognition could take place remotely, covertly and/or from a distance and may produce material with a high degree of sensitive (and surplus) information. Some of the key issues surrounding this development are that biometrics could reveal information such as medical conditions or handicaps, may reveal emotional states or other information that could be perceived as highly intimate by the individual and may result in potential discrimination.

Privacy concerns

Privacy concerns around next-generation biometrics focus on revealing sensitive information and function creep. Specifically, even if second-generation biometrics are linked to less dis-

[1071] McBride, Paul, "Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations", *Journal of Air Law and Commerce*, Vol. 74, No. 3, Summer 2009, pp. 627-662 [p. 659].
[1072] Ibid., p. 661.
[1073] Cronin, David, "Defence cuts people but spends on gadgets", *New Europe*, No. 909, 31 Oct 2010. http://www.neurope.eu/articles/Defence-cuts-people-but-spends-on-gadgets/103501.php
[1074] Hayes, Ben, *Arming Big Brother: the EU's security research programme, Summary of the report*, Transnational Institute, April 2006. http://www.tni.org/es/archives/act/4451
[1075] Whitehead, John W., *Drones Over America: Tyranny at Home*, The Rutherford Institute, Charlottesville, VA, 28 June 2010. http://www.rutherford.org/articles_db/commentary.asp?record_id=661
[1076] Nevins, Joseph, "Robocop: Drones at Home", *Boston Review*, Jan/Feb 2011. http://www.bostonreview.net/BR36.1/nevins.php
[1077] Whitehead, op. cit., 2010.
[1078] Nevins, op. cit., 2011.

tinctive and persistent body traits (such as gait or heat signatures), physiological states or habits may reveal more sensitive information than traditional biometrics, which can be exploited for targeted surveillance and profiling purposes. Some major risks identified by the FIDIS report include discrimination (information used to exclude persons from certain areas), stigmatisation (risk of longer term profiles with negative interpretation) and "unwanted confrontation" (body signals can indicate certain diseases for which medical treatment is unlikely or even impossible).[1079]

Function creep also emerges as an area of specific concern in relation to second-generation biometrics. Function creep occurs when a technology designed for one purpose is used for a completely different purpose. The collection of ancillary and particularly sensitive information by second-generation biometrics may make function creep difficult to resist as behavioural biometrics, soft biometrics and multimodal systems are expected to produce a surplus of information. If this information is centrally stored on a large database, data mining and discriminatory research may occur and enable specific ethnic minorities or other vulnerable groups to be targeted.

Data protection issues

In relation to the Data Protection Directive, biometrics are considered personal information and as such, must be processed in respect of principles such as purpose specification, proportionality, confidentiality and individual consent. According to the EU Data Protection Directive, personal data should always be processed with the user's informed consent; however, some behavioural biometrics can be collected at a distance and without the individual's knowledge. With reference to the individual participation principle, identification procedures pose a greater risk from a data protection perspective when personal data are stored in centralised databases not under full control of the individual. The principle of proportionality is also impacted by behavioural biometrics, which carry the potential to detect people's emotional states or information about their medical history, and multimodal biometric systems, where many different modalities are combined. Finally, many biometric detection systems process sensitive data, for example, data revealing racial or ethnic origin or data concerning health, which must also be processed within strict data protection parameters.

Ethical and social concerns

One of the main philosophical concerns raised by this technology is that biometrics are strictly linked to the human body, whose integrity (physical or psychological) constitutes a key element of human dignity and is protected in the main international legal instruments as a fundamental human right. The human body, as the result of the integration of the physical body and the mind, has a strong symbolic dimension, and is "unavoidably invested with cultural values".[1080] However, the legitimacy of "measuring" the human body as a tool for identifying individuals has been discussed in depth.[1081] One concern raised by scholars has been the increasing "informatization of the body", where the digitalisation of physical and behavioural

[1079] See FIDIS Consortium, *Behavioural Biometric Profiling and Transparency Enhancing Tools*, FIDIS Project, 4 March 2009. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-biometric_profiling_and_transparency_enhancing_tools.pdf

[1080] Mordini Emilio, *Whole Body Imaging at airport checkpoints: the ethical and political context*, HIDE&RISE policy report, February 2010 (updated March 2011). www.riseproject.eu

[1081] Mordini, Emilio and Sonia Massari, "Body, Biometrics and Identity", *Bioethics*, Vol. 22, No. 9, 2008, pp. 488–498. http://www.hideproject.org/downloads/Mordini_Massari-Body_Biometrics_Identity.pdf

attributes of a person and their distribution across the global information network[1082] could affect the representations of ourselves, and may produce processes of disembodiment or body dehumanisation, or offend human dignity[1083]. Scholars have referred to the development of soft, behavioural, electrophysiological biometrics (the so called "under the skin biometrics"), as well as distant and covert data capture potential, as a new step in the informatisation of the body, mainly based on the idea that these systems represent "a significant increase in the extent to which bodies are assumed to become available".[1084]

There is also a significant concern that the widespread use of second-generation biometrics could result in different types of discrimination, resulting from difficulties in enrolment. As biometric applications proliferate, there may be an increasingly presumption that everyone should be enrolled in a biometric system. Ageing emerges as a particular issue for most biometric modalities, where both older people and children may have particular problems in being enrolled; however, injured or disabled groups, people of different racial origins and those with particular medical conditions may also be impacted.[1085] Issues of enrolment could be further exacerbated if biometric identification becomes a key facet of access to social services or travel. Such discrimination is often unintended, but may deeply affect vulnerable individuals and impact on the principle of equality. Furthermore, as discussed above, profiling and function creep can also negatively impact particular groups of individuals.

These different potentials for next-generation biometrics to facilitate discrimination have potential negative impacts on ethical issues such as individual autonomy and self-determination. The collection of very sensitive information revealing medical status, racial origin or other genetic information poses serious concerns over the potential for discrimination against individuals of groups in terms of job opportunities, insurance coverage and public recognition.

9.2.4 Second-generation DNA sequencing technologies

Advances in DNA sequencing technologies allow routine sequencing of the whole genomes of individuals rather than just distinct parts. DNA holds sensitive information about an individual and provides pointers to human qualities that serve as the basis for discrimination and defamation already prevalent in our societies – sex and sexual orientation, societally defined "race", physical and mental health, (absence of specific) talents and gifts, predisposition to aberrant behaviour, aptitude or sustainability for athleticism or employment and eligibility for health, disease or disability.[1086] Given these issues, this case study identified key privacy, data protection, ethical and social issues surrounding second-generation DNA sequencing.

[1082] van der Ploeg, Irma, *The Machine Readable Body: Essays on biometrics and the Informatization of the body*, Shaker, Germany, 2005.

[1083] Mordini Emilio, "Ethics and Policy of biometrics", in M. Tistarelli, Stan Z. Li and Rama Chellappa (eds.), *Handbook of remote biometrics for surveillance and security,* Advances in Pattern Recognition Series, Springer, 2009.

[1084] van der Ploeg Irma, "Security in the danger zone: normative issues of next generation biometrics", in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second Generation Biometrics: the Ethical and Social Context*, Springer, in press.

[1085] Wickins has recently explored the vulnerability of a typical user population falling into six groups, mainly including people with physical or learning disabilities (e.g., spelling problems, walking impairments), people of certain races and religions, those who are elderly or homeless. See Wickins, Jeremy, "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification", *Science and Engineering Ethics*, Vol. 13, No. 1, 2004, pp. 45-54.

[1086] "DNA confidential", *Nature Biotechnology*, Vol. 27, No. 9, 2009, p. 777.

Privacy concerns

One of the primary privacy concerns around the use of second-generation DNA sequencing technologies is the potential for re-identification after de-identification. Despite the assumption that genetic data can be rendered anonymous, it is possible that peoples' identities could be unfolded[1087] and individuals become vulnerable to the consequences of genetic testing, ranging from un-insurability, un-employability or other discrimination or misuse.[1088] There are several actions that could uncover the identity of an individual, such as[1089]:

- Identification by phenotype using imaging techniques for reconstruction of facial features
- Inferring phenotype from genotype by identifying information in DNA and RNA, for instance, stature, hair or iris colour, or skin colour
- Any amount of DNA data in the public domain with a name allows for identification within any anonymised data set

The enormity of whole genome datasets from whole DNA sequencing presents new privacy challenges to researchers, physicians, patients and other related actors. Traditionally, legal frameworks have sought to balance the privacy of data subjects with the benefits of research by relying heavily on informed consent and anonymisation[1090], meaning that the protection of identity of participants is guaranteed by only releasing data in an aggregated form or after identifying variables have been removed.[1091] Re-identification could be possible by using publicly available data and is thereby a threat to privacy.

Furthermore, in addition to identification, but in a similar frame, whole genome DNA sequencing could allow the use of DNA of one family member to provide information about another, which raises an ethical issue of informed consent as well as privacy and data protection. For example, whole genome sequencing could identify when people are related and reveal information about whether another family member has committed a crime or if they are likely to be carriers for particular diseases, etc.[1092]

Data protection issues

A range of data protection issues are also raised by whole genome DNA sequencing. Individuals could be identified by data security breaches, for example:

- When someone hacks into a computer systems where information about DNA samples is stored;
- As a result of physical attacks on encryption keys, for example, so-called cold boot attacks;
- Theft or loss of a laptop or of data-storage devices or IT accidents can lead to security breaches.

[1087] Curren, L., P. Boddington, H. Gowans, N. Hawkins, N. Kanellopoulou, J. Kaye and K. Melham, "Identifiability, genomics and UK data protection law", *European Journal of Health Law*, Vol. 17, No. 4, 2010, pp. 329-344.

[1088] Wjst, M., "Caught you: threats to confidentiality due to the public release of large-scale genetic data sets", *BMC Medical Ethics*, Vol. 11, No.1, 2010, p. 21.

[1089] Lunshof, J.E., R. Chadwick, D. B. Vorhaus and G. M. Church, "From genetic privacy to open consent", *Nature Reviews Genetics*, Vol. 9, No. 5, 2008, pp. 406-411.

[1090] Ibid.

[1091] Heeney, C., N. Hawkins, J. de Vries, P. Boddington and J. Kaye, "Assessing the Privacy Risks of Data Sharing in Genomics", *Public Health Genomics*, Vol. 14, No. 1, 2011, pp. 17-25.

[1092] Hays, Dustin, and DNA Policy Centre, "DNA, Forensics, and the Law", 2008. http://www.dnapolicy.org/policy.issue.php?action=detail&issuebrief_id=42

In relation to the data protection in research contexts, the current framework for protecting informational privacy assumes that the use of genomic datasets would largely be restricted to the scientific research community. However, that is not always true anymore. Also there is no clarity about how evolving results might be best integrated into (electronic) medical records, while protecting data and privacy of the patients.[1093]

With respect to forensics and direct to consumer testing, the storage of data has also emerged as a data protection issue. In forensics, current laws do not always require the destruction of a DNA record or sample after a conviction has been overturned, making it possible that a person's entire genome may be available to law enforcement authorities, researchers or others, regardless of whether they were convicted or not. Although the DNA used for forensic testing is considered non-coding "junk DNA", in the future when the science advances, this information may be found to reveal personal information such as susceptibilities to disease and certain behaviours.[1094] With respect to direct-to-consumer testing, there is no oversight or control regarding how detailed data sets are stored electronically, which presents a data protection threat to individuals whose data is used.[1095]

Ethical and social issues

In addition to privacy and data protection issues, second-generation DNA sequencing raises ethical and social issues. With regard to enabling individuals to be identifiable, the combination of surnames as well as genotype and geographical information could, for example, enable the tracing of an anonymous sperm donor by his offspring in contravention of the law in some jurisdictions. Regarding patient anonymity, there is no consensus on whether there is an obligation to always re-analyse data and provide updated interpretations to patients as new knowledge becomes available. If data were anonymised, patients would not have access to important health information resulting from new discoveries. In this sense, identifiability might be desirable.

Many of the other ethical and social issues relate to consent. In the context of biobanks, existing consent models cannot be assumed to be fully valid anymore and modernised informed consent models addressing novel privacy, ethical and other issues need to be constructed. One particular problem is that information links between disparate parts of human genome information (such as phenotype) could enable the identification of individuals when their consent to research or storage was based upon anonymity. There is also concern about how to obtain appropriate consent if the possible clinical ramifications of testing and storage are not yet fully known or envisioned. Consent protocols must make a careful distinction between the variants in which important clinical observational data exists and those in which disease association is less robust.[1096]

Currently in forensic applications, there is a new "driftnet" approach to comparing scene-of-crime samples against the DNA of the whole population rather than just against that of chosen

[1093] Anderson, M.W., and I Schrijver, "Next Generation DNA Sequencing and the Future of Genomic Medicine", *Genes*, Vol. 1, No. 1, 2010, pp. 38-69.
[1094] Hayes and DNA Policy Centre, 2008.
[1095] Gail, J., "Which way for genetic-test regulation? Assign regulation appropriate to the level of risk", *Nature*, Vol. 466, No. 7308, 2010, pp. 817-818.
[1096] Lunshof, J.E., J. Bobe, J. Aach, M. Angrist, J. V. Thakuria, D. B. Vorhaus, M. R. Hoehe and G. M. Church, "Personal genomes in progress: from the human genome project to the personal genome project", *Dialogues in Clinical Neuroscience*, Vol. 12, No.1, 2010, pp. 47-60.

suspects. For example, in the United Kingdom, all arrested suspects, regardless of the degree of the charge and the possibility that they may not be convicted, can be forced to provide a DNA sample (it is possible for the unconvicted to have their DNA profile removed from the DNA database, although this seems to be an arduous exercise[1097]). This can have negative impacts upon human dignity. Procedures need to be in place to ensure that matches between individuals' DNA profiles and stored DNA profiles do not result in miscarriages of justice. The more DNA profiles compared, the more likely it is that errors will occur and problems will result due to poor laboratory procedures.[1098]

Paternity tests are available commercially, by mail order and through the Internet. Ethical and social concerns include the necessity for informed consent by both parents for a sample to be taken from a child, as a sample from which DNA can be extracted can be obtained from a child by one parent without the other's knowledge. Other issues include ensuring quality control and the availability of counselling after the test result.

Reliability and accuracy also emerge as ethical and social issues. With respect to direct-to-consumer testing, the field is largely unregulated,[1099] and it is uncertain whether all direct-to-consumer genetic tests provide accurate and reliable genotype, sequence and copy-number data. Consequently, there are concerns that patients and consumers could make harmful decisions after receiving incorrect and inadequate information about test results that are provided with little if any involvement of a health-care practitioner. Other concerns include a general uncertainty surrounding regulations governing the return of genomic research results directly to the participants and the impact of false-positive and/or false-negative results.

The case study argues that these diverse concerns and the range of contexts in which they emerge necessitate a sector-specific approach to privacy and data protection in relation to second-generation DNA sequencing.

9.2.4.1 Human enhancement

The human enhancement case study deals with technical and pharmacological human enhancement in light of current concepts of privacy and data protection. Human enhancement can be roughly divided into three fields of application: pharmacological, technical and genetic enhancement. Since DNA-sequencing is already dealt with elsewhere in the PRESCIENT project, this case study focuses on the first two fields of applications. It discusses two technologies: brain computer interfaces (BCIs) and neuro-enhancing pharmaceuticals (neuro-enhancers).

The two most important categorisations of BCIs, particularly in relation to their privacy invasiveness, is their location (invasive vs. non-invasive) and their direction of action, meaning their operation from human to machine and/or vice versa. Although machine-to-human operation can be found in medical applications such as deep brain stimulation, most BCI technology operates from human to machine and is used to image brain activity. Electroencephalography (EEG) that measures the electrical impulses emitted by the brain is the most prevalent

[1097] Mery, David, "How to delete your DNA profile", *The Register*, 7 Jan 2008. http://www.theregister.co.uk/2008/01/07/delete_your_dna_profile/. See also Travis, Alan, "Police told to ignore human rights ruling over DNA database", *The Guardian*, 7 August 2009. http://www.guardian.co.uk/politics/2009/aug/07/dna-database-police-advice
[1098] Lunshof, et al., op. cit., 2010.
[1099] Ibid.

method of displaying brain activity. Although applications such as the mental typewriter or brain-to-robot interfaces are at the moment primarily developed for therapeutic purposes, the gaming and entertainment industry has recently shown an increased interest in the underlying technology.

Neuro-enhancing pharmaceuticals (neuro-enhancers) constitute the second part of the case study. Characterised by their biological and chemical effects, pharmaceutical neuro-enhancement comprise not only illegal drugs (amphetamines or cocaine), but also over-the-counter drugs such as aspirin and prescription drugs (for example, antidepressants and methylphenidate). However, prescription drugs such as Ritalin (methylphenidate) may be misused or used illegally, i.e., by someone other than the person for whom the drug was prescribed. Since the non-prescribed usage of Ritalin is particularly extensive, it serves as an example that is discussed in terms of its privacy-invasive potential.

Pharmacological and technical enhancement affect data protection and privacy in different ways. Privacy is often threatened when the method of enhancement implies the internalisation of substances or technologies (bodily privacy) and/or a potential loss of control. Yet, data protection is only touched upon when a human enhancement technology that is capable of collecting data is involved, regardless of how it may be further processed.

Privacy

Bodily privacy is almost always affected by human enhancement technologies, because they are characterised by the internalisation of technology or bio-chemical substances into the human body. In relation to BCIs, when brain-imaging processes are inverted, i.e. the brain is given an external electrical input, such as in deep brain stimulation processes used in Parkinson's disease treatments, patients can be confronted with a change in their personality. Neuro-enhancers are also problematic in terms of bodily privacy and individual autonomy. Although they represent a softer form of invading one's body in comparison with implantation of technology, their bio-chemical effects still take place inside the human body. Furthermore, the taking of neuro-enhancing drugs can result in the risk of losing control over one's will and actions. Therefore, enhancement drugs such as Ritalin may pose a threat that physicians, parents, employers, etc. can exert external control over the person taking the drug. In addition, unlike BCI technology, neuro-enhancers have successfully entered the mass market and are already having a major impact on today's society.

Data protection

Data protection is primarily impacted by BCI technology, because it is able to collect highly sensitive data. The quality of this data is comparable to genetic information, since the images created by the brain's electrical impulses have an enormous depth of information about the individual, his/her mind and way of thinking. In addition, the amount and type of sensitive information that may be extracted from the data in the future cannot be realistically anticipated. Furthermore, clear legal provisions or guidance determining the sensitive character of BCI data, according to Article 8 of the Data Protection Directive, do not exist. This is particularly problematic, since increasing ways of commercialising BCI data are emerging. Despite this problematic legal situation, system security was apparently given little thought when researchers first developed the technical infrastructure of BCIs, as was the case in the early days of the Internet. Thus, hackers can easily attack BCIs, as shown by the Medical Device Se-

curity Center.[1100] Yet, BCIs are, in many instances, not designed to extract data from the carrier of the technology. Instead, most current BCIs are intended to support people with serious illnesses or disabilities in the communication with or control of other technology.

Ethical and social issues

However, this case study demonstrates that concerns around privacy and data protection are, to a certain extent, subjective and context-dependent. A consideration of the ethical and social aspects of BCIs in particular suggests that when these technologies are used to enhance quality of life, individuals' choices to utilise this technology despite the privacy considerations must be respected. For these individuals, privacy considerations may not take precedence over quality-of-life considerations.

This case study also finds that neither of these technologies is sufficiently regulated in ways that might address the serious privacy, data protection and ethical concerns raised by human enhancement technologies. BCI technology seems to be heavily under-regulated, lacking not only clarity in the legal status of BCI data, but also limits to its implantation into the human body. Additionally, a secure infrastructure between the data subject, the data-collecting device and the computer is missing. In the case of pharmaceutical enhancement, various forms of international and national regulations are in place with regard to controlled substances. However, these substance controls do not provide for protection against the potential privacy invasiveness of neuro-enhancing drugs.

9.3 SYNTHESISING TYPES OF PRIVACY, CASE STUDIES AND PRIVACY IMPACTS

The concept of "privacy" was comprehensively outlined in the first deliverable of this project, where we described the legal, social, economic and ethical dimensions of privacy and data protection. As described in that document, we rely upon Clarke's four different aspects of privacy – privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication[1101] – which we have re-worked into privacy of the person, privacy of data and image, privacy of behaviour and action and privacy of personal communication. We have further expanded these four re-worked dimensions of privacy to also include privacy of thought and feeling, privacy of location and space and privacy of association, including group privacy in order to take account of developments in technology since Clarke identified his four dimensions. Although these seven types of privacy may have some overlaps, they are discussed individually because they provide a number of different lenses through which to view the effects of case study technologies. In the following section, we review these seven types of privacy and match them to information from the case studies.

9.3.1 Privacy of the person

Privacy of the person encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. Privacy of the person is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society. Four of the five case studies we examine, including (1) body scanners, (2) behavioural, physiological and soft biometrics as well as multimodal biometric systems, (3) sec-

[1100] Medical Device Security Center, "Medical Device Security Center", 2011. http://secure-medicine.org/
[1101] Clarke, Roger, "What's 'Privacy'?", Australian Law Reform Commission Workshop, 28 July 2006. http://www.rogerclarke.com/DV/Privacy.html

ond-generation DNA sequencing and (4) brain computer interfaces as well as neuro-enhancing pharmaceuticals all carry the potential to negatively impact upon the privacy of the person.

Body scanners impact the privacy of the person through concerns around the use of body scanners generating images of an individual's naked body, the subsequent revealing of medical information and the improper viewing of such images. Body characteristics such as size and shape of genitals or medical conditions are difficult to keep private when body imaging scanners are used, particularly without PETs such as automated imaging. These scanners may also reveal information about body functions such as colostomy bags or implants.

In relation to second-generation biometrics, bodily privacy could be impacted by the systematic collection of information that could be used for classification purposes such as behaviour, emotion or psychological state. Because of this potential for classification, the *categorisation* of individuals could become a more sensitive issue than *identification* in terms of biometrics, as second-generation biometrics may enable subjects to be characterised via biometric profiling or be used to provide a link to an existing non-biometric profile. Second-generation biometrics also involve the collection of intimate information, which carries the potential to reveal personal data that are classified as sensitive, including medical data, gender, age and/or ethnicity. This could be exacerbated as more, sometimes superfluous, data is collected by multiple biometrics and multimodal systems, in order to improve system performance.

Second-generation DNA sequencing also impacts on the privacy of the person through the collection of intimate information. This intimate information can potentially reveal personal data that are classified as sensitive, as it provides pointers to human qualities that serve as the basis for discrimination and defamation or selection in societies – sex and sexual orientation, societally defined "race", physical and mental health, (absence of specific) talents and gifts, predisposition to aberrant behaviour, aptitude or sustainability for athleticism or employment and eligibility for health, disease or disability. This information could increase the potential for genetic discrimination by government, insurers, employers, schools, banks, and others. Furthermore, genetic data could also potentially identify a person, despite the assumption that it can be rendered anonymous. If these identities were unfolded, individuals could become vulnerable to the consequences of genetic testing ranging from un-insurability, un-employability or other discrimination or misuse. These consequences could affect the individual as well as their family members, due to the heritability of genetic information. In terms of ethics, genetic information in the form of biomarkers is increasingly used to stratify the population into subgroups. Presence or absence of such biomarkers could be used to group a person into a corresponding subgroup, irrespective of the validity of such a correlation.

Human-enhancing technologies may violate privacy of the person, both through brain-computer interfaces and neuro-enhancing pharmaceuticals. For example, someone's bodily privacy could be violated by invasive BCI technology such as deep brain stimulation (used for urgent medical purposes, e.g., treating epilepsy or Parkinson's disease), which could potentially seriously alter one's behaviour and personality. Although neuro-enhancers do not qualify as a technology capable of processing personal data, they can potentially enable the prescribing doctor to exercise control over the recipient, affecting his/her bodily privacy.

9.3.2 Privacy of thoughts and feelings

Our case studies also reveal that new and emerging technologies carry the potential to impact on individuals' privacy of thoughts and feelings. People have a right not to share their thoughts or feelings or to have those thoughts or feeling revealed. Individuals should have the right to think whatever they like. Such creative freedom benefits society because it relates to the balance of power between the state and the individual.[1102] Technologies such as behavioural biometrics and brain-computer interfaces may impact this type of privacy.

Behavioural biometrics can impact privacy of thoughts and feelings through the collection of intimate information that can be used to detect suspicious behaviour or predict malintent. This introduces a concern that human feelings become technically defined and represented and that automated decisions over and about individuals may be made based upon this information.

Furthermore, information from brain computer interfaces may be able to recognise and identify patterns that shed light on certain thoughts and feelings of the carrier.

9.3.3 Privacy of location and space

According to a conception of privacy of location and space, individuals have the right to go wherever they wish (within reason, the prime minister's residence or a nuclear power plant would generally be off-limits), without being tracked or monitored. This conception of privacy also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office. Such a conception of privacy has social value. When citizens are free to go wherever they wish without fear of identification, monitoring or tracking, they experience a sense of living in a democracy and experiencing freedom. Both these subjective feelings contribute to a healthy, well-adjusted democracy. Furthermore, they encourage dissent and freedom of assembly, both of which are essential to a healthy democracy. However, our case studies reveal that technologies such as RFID-enabled travel cards and passports, UASs, embedded biometric systems and behavioural biometrics and second-generation DNA sequencing can negatively impact privacy of location and space.

The case studies describe how RFID-enabled travel cards and e-passports carry the potential for a location threat, whereby individuals' movements can be monitored based on the signature of their RFID-enabled documents. Information about where an individual has been can also be accessed after the fact using information on databases that store information about when and where documents have been read. While this information could be useful for the individual concerned in terms of billing or payment disputes, it may also harm individuals whose location information is revealed to third parties such as police or divorce lawyers. Additionally, the travel card case study indicates that such associations can be spurious in situations where individuals have swapped cards, or when cards have been lost, stolen or cloned.

Case studies also describe how UAS devices can be used to track people or infringe upon their conception of personal space. These surveillance devices can capture images of a person or a vehicle in public space, thereby revealing their location or their movements through public space if more than one image is captured. This information can be used to place individuals in particular places at particular times. UASs can also reveal information about private spaces such as back yards or, when flying low, can even transmit images of activities captured

[1102] Goold, Benjamin J., "Surveillance and the political value of privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009, pp. 3-6.

within homes, offices or other apparently private spaces. The fact that this surveillance can be covert makes the capture of this information particularly problematic.

Second-generation biometrics such as embedded systems and behavioural biometrics may negatively impact privacy of location and space. Sensing and identifying individuals at a distance can result in covert data capture without the data subject's consent. Here, biometrics can be used in tandem with other surveillance systems, such as CCTV, static cameras or mobile phones with location detection capabilities, to pinpoint or track an individual's location.

Whole genome DNA sequencing can also negatively impact on privacy of location and space. This is primarily centred on concerns over the potential for detecting someone's location by comparing the DNA sample found at specific location and people's DNA profiles. This can be grounds for making associations between persons and their location, especially within forensics. It also introduces a possibility for making spurious associations between individuals and particular locations as a result of secondary transfers as this technology becomes more and more sensitive.

9.3.4 *Privacy of data and image*

We expand Clarke's category of privacy of personal data to include the capture of images as these have become considered a type of personal data by the European Union as part of the Data Protection Directive. This privacy of data and image includes concerns about making sure that individuals' data is not automatically available to other individuals and organisations and that they can "exercise a substantial degree of control over that data and its use".[1103] Such control over personal data builds self-confidence and enables individuals to feel empowered. This can be negatively impacted by RFID-enabled travel documents, new surveillance technologies, second-generation biometrics, whole genome DNA sequencing and BCIs. Like privacy of thought and feelings, this aspect of privacy has social value in that it addresses the balance of power between the state and the person.

RFID-enabled travel documents represent a potential threat to privacy of data and image, in that both the travel card and e-passport case studies identified privacy threats associated with the security of RFID systems. This included threats to personal information transmitted in authorised and unauthorised readings of RFID chips as well as threats associated with the security of back-end systems and the personal information stored on databases.

In relation to new technologies of surveillance, body scanners and UASs pose threats to the privacy of data and image. The body scanners case study identified threats regarding the potential for unauthorised or improper viewing, transmitting or storing the naked images of an individual and the effects of this. The UAS case study discussed the fact that UAS surveillance generates images of individuals, sometimes covertly, which leaves individuals no opportunity to avoid such surveillance or access the data held about them.

In terms of second-generation biometrics, behavioural biometrics and the use of biometrics at a distance both pose a threat to personal data or image. Systems that use behavioural biometrics can present a risk of loss of control by data subjects over their personal data. They may not realise that such systems are operating and this could infringe upon their rights to access data that is held about them and to have that data corrected. Behavioural biometrics also

[1103] Clarke, op. cit., 2006.

introduce concerns over the storage of raw data (a person's image or video from cameras monitoring public areas) in databases and how this personal data is used given these new capabilities. As suggested above, the use of biometrics at a distance also introduces issues around consent and transparency, where individuals may not realise systems are in operation.

Whole DNA sequencing technologies may also infringe upon the privacy of a person's data or image. The storage of genomic data without adequate consent in biobanks and databases could be compromised. Furthermore, an individual's phenotypic features (e.g., hair colour, sex, ethnic group, body height) can be derived from genomic data and used for the generation of a rough image of this person. As such, both their personal "data" and their image could be gleaned from gaps in consent and gaps in data protection.

Finally, brain-computer interfaces, as a human enhancement technology, represent a potential threat to personal data in that BCIs involve the digitalisation, collection, (temporary) storage and processing of information about brain activity. This data is highly sensitive, because it contains unique personal information whose prospective worth, especially in terms of its marketing value for the advertisement industry (cf. neuro-marketing), might increase immensely.

9.3.5 Privacy of behaviour and action

We also re-work Clarke's notion of privacy of personal behaviour to privacy of behaviour and action. This concept includes sensitive issues such as sexual preferences and habits, political activities and religious practices. However, the notion of privacy of personal behaviour concerns activities that happen in public space, as well as private space, and Clarke makes a distinction between casual observation of behaviour by a few nearby people in a public space with the systematic recording and storage of information about those activities.[1104] In the first PRESCIENT deliverable, we argued that people have a right to behave as they please (within certain limits, e.g., for example, disrupting the Queen's garden party is off-limits) without having their actions monitored or controlled by others. This benefits individuals in that they are free to do what they like without interference from others which contributes to "the development and exercise of autonomy and freedom in thought and action".[1105] This aspect of privacy can be negatively impacted by RFID-enabled travel documents, new surveillance technologies, behavioural biometrics, whole genome DNA sequencing and human enhancement technologies.

Privacy of behaviour and action can be negatively impacted by RFID-enabled travel documents, in that people's behaviours and travel activities can be reconstructed or inferred from information generated as a result of their use of these technologies. Travel routes, frequent destinations and mode of transport can be gleaned from information available on both e-passport databases and travel card databases. Furthermore, aggregated information can provide details that enable their routines to be inferred.

New surveillance technologies such as body imaging scanners and unmanned aircraft systems can also negatively impact privacy of behaviour and action. Images generated from body scanners could reveal information about behaviour such as augmentation surgeries or medical related practices. With surveillance-oriented UASs, everyone is monitored regardless of whether their activities warrant suspicion; therefore, all behaviours are monitored and re-

[1104] Clarke, op. cit., 2006.
[1105] Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford CA, 2010, p. 82.

corded. Furthermore, the potential to use surveillance covertly means that individuals cannot adjust their behaviour to account for surveillance, unless individuals assume they are being surveilled at all times and attempt to adjust their behaviour accordingly.

Behavioural biometrics potentially impact privacy of behaviour and action primarily through processes of automation. Human behaviour can be monitored, captured, stored and analysed in order to enable systems to become knowledgeable about people. Subsequently, measurements of changes in behaviour and definitions of "abnormal" behaviour become automated. This could lead to monitoring and recording of infrequent behaviours that are not suspicious or criminally deviant. Behavioural biometrics may also impact privacy of behaviour and action by revealing sensitive information about a person's psychological state, which can be used for behaviour prediction.

The advent of whole genome DNA sequencing carries the potential to negatively impact privacy of behaviour and action. As techniques become more sensitive, characteristics in human behaviour may be linked with specific genes and gene sequences. Furthermore, second-generation DNA sequencing might reveal sensitive information on the person's predisposition to certain psychological states and might be used for assessing the predisposition to impaired mental health and aberrant behaviour.

Human enhancement technologies potentially impact upon privacy of behaviour an action in two ways. First, drawing on BCI technology, behavioural neuroscience allows the location of parts of the brain that are supposed to be responsible for certain kinds of behaviour, attitudes and actions. That way, not only would the anticipation of buying behaviour be possible, but also individuals could lose their ability to consent to preventive strategies, such as crime prevention. Second, neuro-enhancers are closely linked to the risk of losing control over one's will and actions. That is why especially prescribed "enhancing" drugs such as Ritalin or modafinil pose a threat of external control (heteronomy) over the individual's behaviour.

9.3.6 Privacy of personal communication

Privacy of personal communications represents the sixth type of privacy which we identify. This aspect of privacy is shared with Clarke, and includes the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages. In the first PRESCIENT deliverable, we argued that people have a right to keep their communications with others private and free from outside monitoring. This benefits individuals because they do not feel inhibited about what they say or feel constantly "on guard" that their communications could be intercepted, monitored or recorded. Society benefits from this aspect of privacy because it enables and encourages a free discussion of a wide range of views and options, and enables growth in the communications sector. This aspect of privacy can be negatively affected by behavioural biometrics and brain-computer interfaces.

Second-generation biometrics, specifically behavioural biometrics, can negatively impact individuals' privacy of personal communications. Speech recognition technologies can be utilised to analyse and disclose the content of communication, and these can be linked with automated systems to ensure that communications by certain individuals, or communications about certain topics, can be monitored or recorded.

This aspect of privacy may also be impacted by brain-computer interfaces, whereby the interception or monitoring of data streams between the BCI user and the machine could be possible.

9.3.7 Privacy of association, including group privacy

Privacy of association, including group privacy, is the final aspect of privacy that we identify. This facet is concerned with people's right to associate with whomever they wish, without being monitored. This has long been recognised as desirable (necessary) for a democratic society as it fosters freedom of speech, including political speech, freedom of worship and other forms of association. Society benefits from this aspect of privacy in that a wide variety of interest groups will be fostered, which may help to ensure that marginalised voices, some of whom will press for more political or economic change, are heard. However, privacy of association can be negatively impacted by technologies such as UASs, behavioural biometrics and second-generation DNA sequencing.

UAS surveillance may impact upon privacy of association through its ability to monitor individuals and crowds, sometimes covertly. Unmanned aircraft systems can also generate information about groups or individuals with whom they associate. For example, at protests or other large gatherings of people, the number and organisation of individuals can be analysed, and group membership can be inferred. If UAS visual surveillance was combined with biometrics such as facial recognition technology, individual group membership and affiliation could be discovered. Furthermore, group activities can also be identified or analysed, for example, place and time of meetings and activities at meetings.

Behavioural biometrics may negatively impact privacy of association. Behavioural biometrics introduces concerns over the potential for the automated creation of categories and allocation of individuals to such categories. Certain types of discrimination could result from this automated allocation, which raises the potential for individual or group profiling.

Second-generation, whole genome sequencing potentially impacts upon privacy of association in negative ways. An individual's presence at a particular location could be detected through linking a person's DNA profile with DNA found at that location. Individuals could be categorised into particular groups based on information gleaned from their DNA sequence. DNA sequencing and profiling makes it possible to monitor groups and individuals and generate sensitive information about the groups or individuals with whom they associate.

9.3.8 Synthesising aspects of privacy

These case studies and the aspects of privacy they may potentially infringe upon are summarised in the table below.

Types of privacy	RFID-enabled travel documents	New surveillance technologies	Second-generation DNA sequencing	Second-generation biometrics	Human enhancement technologies
Privacy of person		✓	✓	✓	✓
Privacy of thought and feelings				✓	✓

Types of privacy	RFID-enabled travel documents	New surveillance technologies	Second-generation DNA sequencing	Second-generation biometrics	Human enhancement technologies
Privacy of location and space	✓	✓	✓	✓	
Privacy of data and image	✓	✓	✓	✓	✓
Privacy of behaviour and action	✓	✓	✓	✓	✓
Privacy of communication				✓	✓
Privacy of association, including group privacy		✓	✓	✓	

Table 9.1: Types of privacy potentially impacted by case study technologies

From the information presented in this chapter and in the table above, we draw various conclusions. First, privacy and data protection are not synonymous. While data protection can be equated with one type of privacy (informational privacy), the concept of privacy is broader than simply data protection. For example, body scanners raise concerns beyond data protection. The introduction of protections from unauthorised viewing of the images, encryption and automated imaging software that used CCTV or generic images of a person did not assuage all of the privacy-related issues around their use. Instead, issues about the generation of naked images, revealing medical conditions and providing alternatives to body scanning whilst protecting the right to travel also emerged as significant issues. Therefore, issues around privacy of the person and privacy around behaviour and action, as well as other ethical concerns had to be considered and adequately addressed before the EC would support their use in EU airports. Any legal or regulatory instrument or set of instruments needs to move beyond data protection impact assessments, which are often only compliance checks, to consider all of the privacy aspects, ethical issues and social concerns that we identify in this document, as well as any others that are emerging or specific to that technology.

Different technologies potentially negatively impact upon different types of privacy. Consolidating the case study information illustrates that privacy of data and image and privacy of behaviour and action are threatened by most if not all new and emerging surveillance technologies. In contrast, privacy of thought and feelings and privacy of communication are potentially impacted by second-generation biometrics and human enhancement technology only. As technologies develop and proliferate, various types of privacy which had not previously been under threat may now be compromised. Therefore, when new technologies are planned and developed, the developers need to consider all of the ways in which a new technology may impact upon privacy, without relying upon a check-list approach that may not capture all types of privacy.

This leads us to our final conclusion that legal or other regulatory instruments will have to be flexible and/or multi-dimensional in order to adequately respond to the heterogeneity of privacy impacts that new technologies introduce. If an assessment of the impacts of a new technology need to take account of the various types of privacy, and be flexible enough to identify

and accommodate previously unconsidered aspects of privacy, then a standard checklist approach to privacy consideration will not suffice. Furthermore, as new uses for existing technologies, or the combination of surveillance technologies in new ways, arise, existing assessments may not consider privacy impacts associated with this use. For example, the DNA sequencing case study argues that data anonymisation may no longer be sufficient to protect privacy if DNA science progresses to the point that individuals may become identifiable based on their DNA sequence in the future. Therefore, in addition to being flexible or multi-dimensional in considering the impacts of introducing technologies, legal, regulatory and/or other instruments will have to be able to account of new uses of technologies. One way in which this could be accomplished is by making instruments or assessments continuous or regular procedures in order to keep pace with changes in technologies.

9.4 THE EXISTING LEGAL FRAMEWORK AND POTENTIAL PRIVACY IMPLICATIONS

The legal chapter in this report also finds that the distinction between legal rights to privacy and data protection must be carried through into the legal context, as the differences between the two resonate through the case studies. First, RFID and new surveillance technologies process data which some might not consider "personal" (i.e., related to an identified or identifiable individual) and thus, should not be subject to data protection legislation. Yet, despite this lack of legal protection for non-personal data, the processing of this data has consequences for the privacy of individuals, for example, in relation to marketing and other practices that introduce discrimination. Second, the legal significance and content of privacy and data protection rights cannot be equated. Both rights contain a proportionality principle, which is embodied in the "necessary in a democratic society" condition in the case of the right to privacy, and is part of the principle of data minimisation in the case of the right to data protection. In respect of the whole genomic sequencing case study, and especially its discussion of genetic biobanks, a proportionality test undertaken from a data protection point of view would yield a more lenient result than that of a proportionality test undertaken from a privacy perspective. Ultimately, this difference can be traced back to the different nature of the two rights, with data protection being a *transparency* tool and privacy being an *opacity* tool. Thus, it is not sufficient for a legal framework to address only one of these rights.

However, the case studies also demonstrate that rights to privacy and data protection should not hinder the development and deployment of new technologies which can significantly benefit individuals. The human enhancement case study emphasises the emancipatory and non-paternalistic nature of the right to privacy, where individuals can experience a significant benefit in terms of quality of life from BCI technology. Because individual self-determination is at the heart of this right to privacy, activities undertaken with an individual's full and informed consent must be considered. This contrasts sharply with the right to data protection, where consent alone does not constitute a legitimate ground for the processing of personal information. Less obviously, the RFID case study also illustrates that individuals can experience benefits, such as ease of travel, from surveillance technologies, if data protection and privacy rights are both considered and addressed throughout the development and deployment of a system.

9.5 CONSIDERING ETHICAL AND SOCIAL ISSUES

Finally, the legal framework also provides an opportunity to consider ethical and social issues alongside the rights to privacy and data protection. These include issues such as human dig-

nity, equality and the rule of law, which encompasses issues of discrimination, consent, self-determination and protection from harm. Furthermore, taking Székely, et al. into account, we understand the "rule of law" as ensuring that the law be predictable, certain, unambiguous and committed to democratic values and individual rights.[1106] In this sense, we understand the "rule of law" as upholding the protections and standards enshrined within the law.

Human dignity

In relation to the principle of human dignity, we find that all five of our case studies potentially infringe upon this principle. In relation to RFID-enabled travel documents, the case study argued that the continuous collection of data from individuals without their knowledge could impact human dignity. The body scanners case study argued that the imperative to undergo body scans that reveal naked images of passengers and/or medical conditions particularly impacts upon human dignity. Further implications for human dignity include the danger that the use of UASs could foster a "Playstation mentality" among operators as they do not see at first-hand the consequences of their actions on the ground. Thus, individuals operating UAS systems as well as those targeted by UAS systems could become de-humanised. Individuals can also become de-humanised by the "informatization of the body"[1107], whereby the digitalisation of physical and behavioural attributes could affect our representations of ourselves and impact upon human dignity, primarily because the body is attached to strong cultural values. In relation to second-generation DNA sequencing human dignity in health care could be impacted if principles of anonymisation mean that individuals are not informed about new information regarding their disease risk profiles. Also in the DNA case study, requiring people arrested for certain crimes to give DNA samples, and by proxy, requiring family members of those individuals to reveal DNA information negatively affects human dignity as well as autonomy. Finally, the human enhancement case study argued that individuals have a right to self-determination as part of human dignity, which means that their informed consent to use BCIs, despite the privacy concerns, should be respected.

Equality

The RFID, body scanners, second generation DNA sequencing and second-generation biometrics case studies all raised issues surrounding intentional or un-intentional discrimination against particular population groups. In terms of RFID, this included the potential for power differentials between those operating RFID travel card systems and those who carry the cards. As a result, data processers can categorise individuals into particular profiles and this could result in a denial of service. The body scanners case study also identified the potential for religious discrimination, where religious Jewish and Muslim women who placed a premium on personal modesty were being discriminated against by compulsory body scanning policies. Information from the second-generation biometric case study also identified discriminatory effects in relation to older people, children, those with certain medical conditions or disabilities and/or those of particular racial backgrounds for whom it is known that biometrics are less accurate. This could result in these groups being less able to access services; particularly state services as biometrics become more widely deployed. Finally, in relation to the DNA case study, individuals may be discriminated against as DNA information becomes increasingly able to reveal information about social or (eventually possibly) psychological characteristics such as "race" or personality characteristics that could result in discrimination. Further-

[1106] Székely, Ivan, Máté Dániel Szabó and Beatrix Vissy, "Regulating the future? Law, ethics, and emerging technologies", *Journal of Information, Communication & Ethics in Society*, Vol. 9, No. 3, 2011, pp. 180-194.
[1107] van der Ploeg, op. cit., 2005.

more, family members of those who are arrested may become discriminated against as a result of information about them that is revealed by their family member's DNA.

The rule of law

With regard to the rule of law, our case studies also identified potential ethical or social impacts. The RFID case studies identified the potential for identity theft, where some RFID systems did not secure personal data enough to protect individuals from harm. The consequences of identity theft could include an individual being denied a job or the ability to get bank credit, which could significantly affect their life chances. The body scanners case study argued that these devices interfered with an individual's right to travel and their religious freedom in some contexts where body scanning was a requirement to fly with no alternative, for example, a pat down search. Stakeholders quoted in the UAS case study commented that these devices represented a generalised threat to freedom and civil liberties. However, both the UAS and second-generation biometrics case studies argued that the deployment of these devices "at a distance" negatively impacted upon people's ability to consent to the collection and processing of their data as required by the EU Data Protection Directive. Consent is also impacted in the second-generation DNA sequencing case study by Internet and direct-to-consumer testing, particularly with regard to paternity testing, which can be done covertly and without the consent of the other parent. The DNA case study also recognised that second-generation sequencing may not adequately address the data protection principle of anonymity if individuals can be re-identified from sophisticated DNA sequencing techniques.

Given these significant impacts on ethics and social issues, as well as privacy and data protection, the following section outlines policy recommendations that would enable policy-makers to ensure that these issues are adequately considered in the development and deployment of new and emerging surveillance technologies.

9.6 POLICY RECOMMENDATIONS

This synthesis of case study information around potential privacy impacts, ethical impacts and the extent to which the current regulatory regime addresses these impacts suggests two different policy recommendations regarding the use of new and emerging surveillance technologies. Broadly, we argue that privacy, data protection and ethical and social issues are not commensurate, and that new legislation needs to account for negative impacts associated with all three of these. Privacy impact assessments offer the most appropriate avenue for comprehensively addressing all three of these potential impacts without encountering the inflexibility of over-arching legislation.

The case studies examined here demonstrate that a focus on data protection will not address all of the negative impacts associated with the introduction of new technologies. The case studies indicate that vague, high-level data protection limitations, such as data anonymisation or data minimisation, do not accurately reflect the reality of the effects of new and emerging technologies. These new technologies impact upon multiple dimensions of privacy, ethical and social issues alongside their potential impacts on data protection. In addition to data protection issues surrounding consent and data minimisation, other types of privacy issues emerge. For example, body scanners raise bodily privacy issues, while BCIs or second-generation biometrics raise issues around the privacy of thoughts and feelings. Also, data protection principles such as anonymisation may actually raise ethical problems, such as when individuals' DNA reveals a propensity to develop certain diseases. Regulatory mechanisms

also need to account for rule of law aspects such as providing viable alternatives to surveillance that do not impact on people's ability to exercise other rights. Individuals should be free to meet, communicate and interact with any individuals or organisations that they wish without being subject to monitoring by surveillance technologies. Individuals should also be free to move about in public space or travel across borders without submitting their bodies to automated surveillance by new and emerging technologies. On a legislative level, the case study data indicated that it is important to harmonise privacy and data protection legislation across the individual Member States and within the EU. The EC is already considering a revision to the Data Protection Directive, including improvements that would harmonise many issues across Member States.[1108] Specific aspects being considered for harmonisation include consent, data minimisation, storage limitations, use limitations and rights of access and correction. This legislation may also be over-arching in that it will apply to the commercial sector and public organisations or authorities, such as universities, police, immigration authorities or other public bodies. These improvements may also address some of the gaps associated with focusing on data protection without considering some of the complex privacy and ethical issues that new technologies introduce. Specifically, these changes may broaden the scope of the legislation from data protection to include other aspects of technology assessment. One particular facet of these proposed changes include the mandatory undertaking of privacy impact assessments (PIAs) for the introduction of new technologies or systems, or when systems are substantially re-organised.

The introduction of mandatory PIAs would enable organisations to account for the complexity of new technologies, their increasing capabilities, their applications, the sectors in which they are deployed and their impacts on a range of data protection, privacy and ethical issues. Using PIAs, privacy, data protection and ethical considerations would be built in to the whole process of technology development and deployment. As Wright argues, a mandatory PIA would:

> complement data protection legislation and help to increase awareness of the exigencies and obligations imposed by such legislation [and encourage] high levels of accountability and transparency[, which] are vital to the way organizations handle and share personal information.[1109]

However, some have criticised PIAs for their focus on privacy to the detriment of other considerations such as ethical or social issues. Raab and Wright argue that this can be rectified by a pluralistic approach that captures the various ethical, social and other "meanings and associations within privacy's conceptual family".[1110] Mechanisms such as pluralistic privacy impact assessments would encourage organisations to consider a variety of privacy, data protection, ethical and social risks and how these can be adequately addressed, rather than simply complying with a checklist of data protection principles. Furthermore, privacy impact assessments that are regularly updated enable organisations to anticipate further changes in technology capabilities or applications. Legal regulation should also include adequate redress mechanisms and meaningful sanctions for organisations or bodies which do not comply with relevant data protection principles and codes of conduct. These legal mechanisms should be harmonised across the EU to ensure that all organisations adhere to similarly high standards of privacy, data, ethical and social protections.

[1108] European Commission, Communication A comprehensive approach on personal data protection in the European Union, (2010) 609 final, 4 Nov 2010.

[1109] Wright, David, "Should Privacy Impact Assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011, pp. 121-131, [p. 128].

[1110] Raab, Charles and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

9.7 REFERENCES

American Civil Liberties Union (ACLU), "The ACLU's view on body scanners", 15 Mar 2002. http://www.aclu.org/technology-and-liberty/body-scanners

American Civil Liberties Union (ACLU), "Backgrounder on Body Scanners and 'Virtual Strip Searches'", 8 Jan 2010. http://www.aclu.org/technology-and-liberty/aclu-backgrounder-body-scanners-and-virtual-strip-searches

Anderson, M.W., and I Schrijver, "Next Generation DNA Sequencing and the Future of Genomic Medicine", *Genes*, Vol. 1, No. 1, 2010, pp. 38-69.

Bloomfield, Steve, "How an Oyster Card can Ruin your Marriage", *The Independent on Sunday*, 19 Feb 2006. http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html

Bronk, Christopher, *Innovation By Policy: A Study of the Electronic Passport*, 2007. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1557728

Buchmann, J., A. May and U. Vollmer, "Perspectives for Cryptographic Long-Term Security," *Communications of the ACM*, Vol. 49, No. 9, 2006.

Clarke, Roger, "What's 'Privacy'?", Australian Law Reform Commission Workshop, 28 July 2006. http://www.rogerclarke.com/DV/Privacy.html

CBC News, "Airport scanners invade privacy: advocate", 5 Jan 2010. http://www.cbc.ca/canada/british-columbia/story/2010/01/05/bc-airport-scanners-civil-liberties-vonn.html

Cronin, David, "Defence cuts people but spends on gadgets", *New Europe*, No. 909, 31 Oct 2010. http://www.neurope.eu/articles/Defence-cuts-people-but-spends-on-gadgets/103501.php

Curren, L., P. Boddington, H. Gowans, N. Hawkins, N. Kanellopoulou, J. Kaye and K. Melham, "Identifiability, genomics and UK data protection law", *European Journal of Health Law*, Vol. 17, No. 4, 2010, pp. 329-344.

Department for Transport, *Impact Assessment on the use of security scanners at UK airports*, 29 Mar 2001.

The Economist, "Unmanned aircraft: The fly's a spy", 1 Nov 2007. http://www.economist.com/displaystory.cfm?story_id=10059596

Electronic Privacy Information Center (EPIC), "Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding", June 2005. http://epic.org/privacy/surveillance/spotlight/0605/

EPIC, *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking, Spotlight on Surveillance*, August 2005. http://epic.org/privacy/surveillance/spotlight/0805/

European Commission, Communication: A comprehensive approach on personal data protection in the European Union, (2010) 609 final, 4 Nov 2010.

European Economic and Social Committee, Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM(2010) 311 final, Brussels, 16 Feb 2011.

FIDIS Consortium, *Behavioural Biometric Profiling and Transparency Enhancing Tools*, FIDIS Project, 4 March 2009. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-biometric_profiling_and_transparency_enhancing_tools.pdf

Gail, J., "Which way for genetic-test regulation? Assign regulation appropriate to the level of risk", *Nature*, Vol. 466, No. 7308, 2010, pp. 817-818.

The Guardian, "Oyster data use rises in crime clampdown", 13 Mar 2006. http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation

Hayes, Ben, *Arming Big Brother: the EU's security research programme, Summary of the report*, Transnational Institute, April 2006. http://www.tni.org/es/archives/act/4451

Hays, Dustin, and DNA Policy Centre, *DNA, Forensics, and the Law*, 2008.

Heeney, C., N. Hawkins, J. de Vries, P. Boddington and J. Kaye, "Assessing the Privacy Risks of Data Sharing in Genomics", *Public Health Genomics*, Vol. 14, No. 1, 2011, pp. 17-25.

Henrici, Dirk, *RFID Security and Privacy – Concepts, Protocols, and Architectures*, Springer, Berlin, 2008.

Heussner, Ki Mae, "Air Security: Could Technology Have Stopped Christmas Attack?", *ABC News*, 29 Dec. 2009. http://abcnews.go.com/Technology/AheadoftheCurve/air-security-technology-stopped-xmas-attack/story?id=9436877

Hornung, G., *The European regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, 2007. http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.asp

Hull, Liz, "Drone makes first UK 'arrest' as police catch car thief hiding under bushes", *Daily Mail*, 12 Feb 2010. http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html#ixzz1JV7EKR1N

Juels, Ari, David Molnar, and David Wagner, "Security and Privacy Issues in E-passports", *Security and Privacy for Emerging Areas in Communications Networks,* 2005.

Klitou, Demetrius, "Backscatter body scanners – A strip search by other means", *Computer Law & Security Report*, Vol. 24, Issue 4, 2008, pp. 316-325.

Lunshof, J.E., C. Ruth, B.V. Daniel and M. C. George, "From genetic privacy to open consent", *Nature Reviews Genetics*, Vol. 9, No. 5, 2008, pp. 406-411.

Lunshof, J.E., J. Bobe, J. Aach, M. Angrist, J. V. Thakuria, D. B. Vorhaus, M. R. Hoehe and G.M. Church, "Personal genomes in progress: from the human genome project to the personal genome project", *Dialogues in Clinical Neuroscience*, Vol. 12, No.1, 2010, pp. 47-60.

McBride, Paul, "Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations", *Journal of Air Law and Commerce*, Vol. 74, 2009.

Mason, Wyatt, "Scanners Gone Wild", *The New York Times*, 3 Dec 2010. http://www.nytimes.com/2010/12/05/magazine/05FOB-wwln-t.html?ref=technology

Medical Device Security Center, "Medical Device Security Center", 2011. http://secure-medicine.org/

Mery, David, "How to delete your DNA profile", *The Register*, 7 Jan 2008. http://www.theregister.co.uk/2008/01/07/delete_your_dna_profile/

Miller, Vikki, "Oyster card: fears over Mifare security", *The Telegraph*, 21 June 2008. http://www.telegraph.co.uk/news/newstopics/politics/2168791/Oyster-card-fears-over-Mifare-security.html

Mordini, Emilio, *Whole Body Imaging at airport checkpoints: the ethical and political context*, HIDE & RISE policy report, February 2010 (updated March 2011). www.riseproject.eu

Mordini, Emilio, "Ethics and Policy of biometrics", in M. Tistarelli, Stan Z. Li, Rama Chellappa (eds.), *Handbook of remote biometrics for surveillance and security,* Advances in Pattern Recognition Series, Springer, 2009.

Mordini, Emilio, and Sonia Massari, "Body, Biometrics and Identity", *Bioethics*, Vol. 22, No. 9, 2008, pp. 488–498. http://www.hideproject.org/downloads/Mordini_Massari-Body_Biometrics_Identity.pdf

Nature Biotechnology, "DNA confidential", Vol. 27, No. 9, 2009.

Nevins, Joseph, "Robocop: Drones at Home", *Boston Review*, Jan/Feb 2011. http://www.bostonreview.net/BR36.1/nevins.php

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford CA, 2010.

Organisation for Economic Cooperation and Development, "RFID Guidance and Reports", *OECD Digital Economy Papers*, No. 152, OECD publishing, 2008.

Privacy International, "PI statement on proposed deployments of body scanners in airports", 31 Dec 2009. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-

Quinn, Ben, "Why Europe doesn't want an invasion of body scanners", *Christian Science Monitor*, 26 Jan 2010. http://www.csmonitor.com/World/Europe/2010/0126/Why-Europe-doesn-t-want-an-invasion-of-body-scanners

Raab, Charles and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

Randerson, James, "Eye in the sky: police use drone to spy on V festival", *The Guardian*, 21 Aug 2007. http://www.guardian.co.uk/uk/2007/aug/21/ukcrime.musicnews

Rucker, Philip, "US airports say seeing is believing as passengers face body-scan drill", *Sydney Morning Herald*, 5 Jan 2010. http://www.smh.com.au/travel/travel-news/us-airports-say-seeing-is-believing-as-passengers-face-bodyscan-drill-20100104-lq6o.html

Sia, Richard H.P., "Agencies see homeland security role for surveillance drones", *Congress-Daily*, 12 Dec 2002. http://www.govexec.com/dailyfed/1202/121202sia.htm

Spiekermann, Sarah, *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*, Shaker Verlag, Aachen, 2008.

Srivastava, Lara, "Radio frequency identification: ubiquity for humanity", *info*, Vol. 9, No. 1, 2007, pp. 4-14.

Stajano, F., L. Bianchi, P. Li and D. Korff, "Forensic genomics: Kin privacy, driftnets and other open questions", *Proceedings of the 2008 ACM Workshop on Privacy in the Electronic Society*, 2008.

Székely, Ivan, Máté Dániel Szabó and Beatrix Vissy, "Regulating the future? Law, ethics, and emerging technologies", *Journal of Information, Communication & Ethics in Society*, Vol. 9, No. 3, 2011, pp. 180-194.

Travis, Alan, "Police told to ignore human rights ruling over DNA database", *The Guardian*, 7 August 2009. http://www.guardian.co.uk/politics/2009/aug/07/dna-database-police-advice

van der Ploeg Irma, "Security in the danger zone: normative issues of next generation biometrics", in Emilio Mordini and Dmitrios Tzovaras (eds.), *Second Generation Biometrics: the Ethical and Social Context*, Springer, in press.

van der Ploeg, Irma, *The Machine Readable Body: Essays on biometrics and the Informatization of the body*, Shaker, Germany, 2005.

van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij and Claudio Borean, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, Office for Official Publications of the European Communities, Luxembourg, 2007.

Whitehead, John W., *Drones Over America: Tyranny at Home*, The Rutherford Institute, Charlottesville, VA, 28 June 2010. http://www.rutherford.org/articles_db/commentary.asp?record_id=661

Wickins, Jeremy, "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification", *Science and Engineering Ethics*, Vol. 13, No. 1, 2004, pp. 45-54.

Wjst, M., "Caught you: threats to confidentiality due to the public release of large-scale genetic data sets", *BMC Medical Ethics*, Vol. 11, No.1, 2010.

Wright, David, "Should Privacy Impact Assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011, pp. 121-131.
Wright, David, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].
Zetter, Kim, "Airport Scanners Can Store, Transmit Images", *Wired News*, 11 January 2010. http://www.wired.com/threatlevel/2010/01/airport-scanners/