2013

Seven Types of Privacy

Rachel L. Finn
David Wright
Michael Friedewald, *Fraunhofer Institute for Systems and Innovation Research*

Seven types of privacy

Rachel Finn and David Wright, Trilateral Research & Consulting, London
Michael Friedewald, Fraunhofer ISI, Karlsruhe

1 INTRODUCTION

Theoretical and legal conversations about the relationship between technology and privacy date back to the 1890s with the advent of portable photography equipment accessible to the general population.[1] As technologies continue to develop, conceptualisations of privacy have developed alongside them, from a "right to be let alone" to attempts to capture the complexity of privacy issues within frameworks that highlight the legal, social-psychological, economic or political concerns that technologies present. However, this reactive highlighting of concerns or intrusions does not provide an adequate framework though which to understand the ways in which privacy should be proactively protected. Rights to privacy, such as those enshrined in the European Charter of Fundamental Rights, require a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions, infringements and problems. One such framework is presented by Roger Clarke, who, in the mid-1990s, identified four different categories of privacy, which enabled him to outline specific protections.[2]

Clarke was the first privacy scholar of whom we are aware to have categorised the types of privacy in a logical, structured, coherent way. Others, such as Solove, have also developed a taxonomy of privacy.[3] However, Solove's taxonomy focuses on privacy harms rather than characterising the types of privacy.

Since Clarke's conceptualisation, new and emerging technologies have introduced further privacy effects, and Clarke's four categories are no longer adequate to address the concerns they introduce. This paper makes a contribution to a forward-looking privacy framework by examining the privacy impacts of six new and emerging technologies. It analyses the privacy issues that each of these technologies present and argues that despite his initial capturing of the heterogeneity of privacy categories, Clarke's taxonomy must be revised and expanded to include seven different types of privacy. We also use this case study information to suggest that an imprecise conceptualisation of privacy may be necessary to maintain a fluidity that enables new dimensions of privacy to be identified, understood and addressed in order to effectively respond to rapid technological evolution.

---

[1] Samuel Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890).

[2] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" (Xamax Consultancy, Aug 1997). http://www.rogerclarke.com/DV/Intro.html. Clarke identified these four categories even earlier, in his PhD Supplication in 1995. See http://www.rogerclarke.com/DV/PhD.html. He has variously referred to the four categories as categories, interests, dimensions, components and aspects. We use the term "types", which Gary T. Marx also uses. See Gary T. Marx, "Privacy is not quite like the weather" in *Privacy Impact Assessment*, edited by David Wright and Paul De Hert (Dordrecht: Springer, 2012).

[3] See Daniel Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008).

To be published in:
S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,DOI 10.1007/978-94-007-5170-5_1,

2 DEFINING AND CONCEPTUALISING PRIVACY

"Privacy" is a key lens though which many new technologies, and most especially new surveillance technologies, are critiqued.[4] However, "privacy" has proved notoriously difficult to define. Serge Gutwirth says "The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as "our" privacy, it still finds a way to remain elusive."[5] Colin Bennett notes that "attempts to define the concept of 'privacy' have generally not met with any success".[6] Legal scholars James Whitman and Daniel Solove have respectively described privacy as "an unusually slippery concept"[7], and "a concept in disarray. Nobody can articulate what it means"[8]. Furthermore, Debbie Kaspar notes that "scholars have a famously difficult time pinning down the meaning of such a widely used term [and] …most introduce their work by citing this difficulty".[9] Helen Nissenbaum has argued that privacy is best understood though a notion of "contextual integrity", where it is not the sharing of information that is a problem, rather it is the sharing of information outside of socially agreed contextual boundaries.[10] Political scientists have also discussed privacy in relation to state power, arguing that privacy has to be understood in connection to the other political rights that it allows individuals to exercise by protecting autonomy.[11] Others have focused on the economics of privacy, discussing how privacy is threaded through economic inequality, capitalism and private property. Christian Fuchs argues that in the economic context privacy is beneficial to companies and wealthy individuals because it masks income inequality, while privacy is simultaneously undermined by these very same companies who seek to control workers and consumers.[12] Feminist scholars have traced the ways in which appeals to privacy have been used to supported and reinforce gender inequality.[13] Still other scholars have pointed out that privacy has a social value as well and, indeed, is a bedrock of democracy itself.[14] Gutwirth explains why: privacy is "a cornerstone of contemporary Western society because it affects individual self-determination; the autonomy of relationships; behavioural independence; existential choices

---

[4] David Lyon, *Surveillance after September 11* (Cambridge: Polity Press, 2003).
[5] Serge Gutwirth, *Privacy and the information age* (Lanham, MD: Rowman & Littlefield, 2002), 30.
[6] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca NY: Cornell University Press, 1992).
[7] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," *The Yale Law Journal* 113 (2004): 1153-54.
[8] Solove, 12. Solove believes that privacy is not one thing, that there is no common dominator. We can agree with that – in so far as we have identified seven types of privacy. However, we believe that there *is* a common denominator and that common denominator is the ill-defined notion of privacy itself. While we agree with Gutwirth, Priscilla Regan and others who say that privacy has a social value, privacy at its core relates to the integrity and autonomy of the individual, so that when privacy is compromised – no matter what type of privacy – the individual is being harmed in some way.
[9] Debbie V. S. Kaspar, "The Evolution (or Devolution) of Privacy," *Sociological Forum* 20 (2005): 72.
[10] Helen Nissenbaum, "Privacy as Contextual Integrity", *Washington Law Review,* 79:1 (2004), 101-139.
[11] Benjamin J. Goold, "Surveillance and the Political Value of Privacy," *Amsterdam Law Forum* 1 (2009): 5.
[12] Christian Fuchs, "Towards an alternative concept of privacy," *Journal of Information, Communication and Ethics in Society* 9 (2011): 232.
[13] Catharine A. MacKinnon, *Feminism Unmodified: Discourses on Life and Law* (Cambridge MA: Harvard University Press, 1987).
[14] The Supreme Court of Canada has stated that "society has come to realize that privacy is at the heart of liberty in a modern state." R. v. Dyment (188), 55 D.L.R. (4th) 503 at 513 (S.C.C.). On the social value of privacy, see, for example, Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy, (*Chapel Hill, University of North Carolina Press, 1995), 220-231; Alan Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, 59: 2 (2003), 431-453; Valerie Steeves, "Reclaiming the social value of privacy", in Ian Kerr, Valerie Steeves and Carole Lucock (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, 2009).

and the development of one's self; spiritual peace of mind and the ability to resist power and behavioural manipulation."[15]

Although a widely accepted definition of privacy remains elusive, there has been more consensus on a recognition that privacy comprises multiple dimensions, and some privacy theorists have attempted to create taxonomies of privacy problems, intrusions or categories. For example, Solove asserts that privacy is best understood as a "family of different yet related things"[16]. Solove arrives at this conclusion by outlining a taxonomy of privacy problems that must be addressed, regardless of whether they conform to a precise definition of privacy. His taxonomy includes problems related to *information collection*, such as surveillance or interrogation, problems associated with *information processing*, including aggregation, data insecurity, potential identification, secondary use and exclusion, *information dissemination*, including exposure, disclosure breach of confidentiality, etc. and *invasion*, such as issues related to intrusion and decisional interference.[17] A typology of privacy intrusions is also offered by Debbie Kaspar, who argues that privacy cannot be understood unless examined from the inside. Kaspar distinguishes between invasions involving extraction, observation and intrusion.[18] *Extraction*-based privacy invasions involve making a deliberate effort to obtain something from a person. *Observation*-based privacy invasions are characterised by active and on-going surveillance of a person, while *intrusion*-based invasions involve an "unwelcome presence or interference" in a person's life.[19]

However, these scholars' focus on the ways in which privacy can be infringed and the legal problem which must be solved is largely reactive. They focus on specific harms which are already occurring and which must be stopped, rather than over-arching protections that should be instituted to prevent harms. The difference between a taxonomy of privacy harms and a taxonomy of types of privacy is the pro-active, protective nature of the latter. It's the difference between outlawing murder and adopting a right to life. Murder is only one way in which life can be undermined, and a simple prohibition against murder would enable the dissolution of safety principles, etc. Instead, a positive right to life forces individuals, governments and other organisations to evaluate how their activities may impact upon a right to life and introduce protective measures.

Roger Clarke's human-centred approach to defining categories of privacy does assist in outlining what specific elements of privacy are important and must be protected. Clarke's four categories of privacy, outlined in 1997, include privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication.[20] *Privacy of the person* has also been referred to as "bodily privacy" and is specifically related to the integrity of a person's body. It would include protections against physical intrusions, including torture, medical treatment, the "compulsory provision of samples of body fluids and body tissue" and imperatives to submit to biometric measurement. For Clarke, privacy of the person is thread through many medical and surveillance technologies and practices. *Privacy of personal behaviour* includes a protection against the disclosure of sensitive

[15] Gutwirth, *Privacy and the information age*.
[16] Solove, *Understanding Privacy*, 9.
[17] Daniel Solve, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* 44 (2007): 758.
[18] Kaspar, *Evolution of Privacy*, 76.
[19] Ibid.
[20] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997. http://www.rogerclarke.com/DV/Intro.html

personal matters such as religious practices, sexual practices or political activities. Clarke notes that there is a space element included within privacy of personal behaviour, where people have a right to private space to carry out particular activities, as well as a right to be free from systematic monitoring in public space. *Privacy of personal communication* refers to a restriction on monitoring telephone, e-mail and virtual communications as well as face-to-face communications through hidden microphones. Finally, *privacy of personal data* refers to data protection issues. Clarke adds that, with the close coupling that has occurred between computing and communications, particularly since the 1980s, the last two aspects have become closely linked, and are commonly referred to as "information privacy".

3 SEVEN TYPES OF PRIVACY

Despite the utility of these four categories, recent technological advances have meant that they are no longer adequate to capture the range of potential privacy issues which must be addressed. Specifically, technologies such as whole body imaging scanners, RFID-enabled travel documents, unmanned aerial vehicles, second-generation DNA sequencing technologies, human enhancement technologies and second-generation biometrics raise additional privacy issues, which necessitate an expansion of Clarke's four categories. We will use these new and emerging technologies to argue for an expansion to seven different types of privacy, including privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy).[21] 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 this section, we briefly outline each of these seven types of privacy before linking them with relevant information from new and emerging technologies in the next section.

Privacy of the person encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. According to Mordini, the human body has a strong symbolic dimension as the result of the integration of the physical body and the mind and is "unavoidably invested with cultural values".[22] Privacy of the person is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society. This aspect of privacy is shared with Clarke's categorisation.

We extend 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.[23] The ability to behave in public, semi-public or one's private space without having actions monitored or

[21] These seven types of privacy were first elaborated in an annex prepared for the PRESCIENT D1 report, available at http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf

[22] Emilio Mordini, "Whole Body Imaging at airport checkpoints: the ethical and political context", in *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, ed. René von Schomberg (Luxembourg: Publications Office of the European Union, 2011).

[23] Clarke, "Introduction to Dataveillance".

controlled by others contributes to "the development and exercise of autonomy and freedom in thought and action".[24]

Privacy of communication aims to avoid 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. This right is recognised by many governments through requirements that wiretapping or other communication interception must be overseen by a judicial or other authority. This aspect of privacy benefits individuals and society because it enables and encourages a free discussion of a wide range of views and options, and enables growth in the communications sector.

We expand Clarke's category of privacy of personal data to include the capture of images as these are considered a type of personal data by the European Union as part of the 1995 Data Protection Directive as well as other sources. 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 people can "exercise a substantial degree of control over that data and its use".[25] Such control over personal data builds self-confidence and enables individuals to feel empowered. 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.

Our case studies 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.[26] This aspect of privacy may be coming under threat as a direct result of new and emerging technologies.[27] Privacy of thought and feelings can be distinguished from privacy of the person, in the same way that the mind can be distinguished from the body. Similarly, we can (and do) distinguish between thought, feelings and behaviour. Thought does not automatically translate into behaviour. Similarly, one can behave thoughtlessly (as many people often do).

According to our conception of **privacy of location and space**, individuals have the right to move about in public or semi-public space without being identified, 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 move about public space 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. This categorisation of privacy was also not as obviously under threat when Clarke was writing in 1997, however, this has changed with technological advances.

The final type of privacy that we identify, **privacy of association (including group privacy)**, is concerned with people's right to associate with whomever they wish, without

[24] Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford CA: Stanford University Press, 2010), 82.
[25] Clarke, "Introduction to Dataveillance".
[26] Goold, "Surveillance and the Political Value of Privacy".
[27] See Dara Hallinan and Paul De Hert, "Neurodata Based Devices and Data Protection", 2012 [forthcoming].

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. This aspect of privacy was not considered by Clarke, and a number of new technologies outlined below could negatively impact upon individuals' privacy of association.

One might question what the difference is between privacy of location and space or privacy of association and privacy of behaviour. Privacy of location means that a person is entitled to move through physical space, to travel where she wants without being tracked and monitored. Privacy of behaviour means the person has a right to behave as she wants (to sleep in class, to wear funny clothes) so long as the behaviour does not harm someone else. Privacy of behaviour does not necessarily have anything to do with a person travelling through space, driving to work, going shopping or whatever. One can behave as one wants in private, separately from others. Privacy of association differs from privacy of behaviour because it is not only about groups or organisations (e.g., political parties, trade unions, religious groups, etc.) to which we choose to belong, privacy of association also connects to groupings or profiles over which we have no control – for example, DNA testing can revealing that we are members of a particular ethnic group or a particular family. Privacy of association directly relates to other fundamental rights such as freedom of religion, freedom of assembly, etc., from which privacy of behaviour and action (as we define it) are a step removed.

Our typology of privacy (or, rather, our expansion of Clarke's typology) offers various benefits to a range of stakeholders. It is important above all in policy terms, i.e., policy-makers should ensure that these different types of privacy are adequately protected in legislation, i.e., it is not sufficient to protect only personal data and personal communications (e.g., against interception). This typology is also of instrumental value in the development of a privacy impact assessment methodology in Europe (as is being done in the EC-funded PIAF[28], PRESCIENT[29] and SAPIENT[30] projects, for example). Similarly, organisations that carry out privacy impact assessments should be concerned not only about privacy of personal data and privacy of communications, but also the other types of privacy as well. We also believe our typology provides academics and other privacy experts with a useful, logical, well-structured and coherent typology in which to frame their privacy studies. Our typology is similarly useful for privacy advocates. Although a widely accepted definition of privacy has proven elusive, this typology, firmly building on that established by Clarke, should be widely accepted.

4 PRIVACY IMPACTS OF NEW AND EMERGING TECHNOLOGIES

In this section, we discuss six new and emerging technologies and their potential impact upon the seven different types of privacy outlined above. We use whole body imaging scanners, RFID-enabled travel documents, unmanned aircraft systems (drones), second-generation DNA sequencing, human enhancement technologies and second-generation biometrics to illustrate the need to expand Clarke's four categories. For each technology, we examine what types of privacy they could infringe upon. We demonstrate that different technologies impact upon different types of privacy and that technological developments can introduce new and

[28] www.piafproject.eu
[29] www.prescient-project.eu
[30] www.sapientproject.eu

unforeseen facets of privacy. We also analyse these several new and emerging technologies in terms of their impact on one or more different types of privacy in order to assist policy-makers in understanding these new additional types of privacy and in devising protections that address all of these different types.

4.1 WHOLE BODY IMAGING SCANNERS

Whole body imaging scanners 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 that law enforcement and security staff need tools to enable them to deal with threats from explosives and non-metallic weapons.[31] 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.[32] Given the sensitive nature of the images produced by body scanners, critics have raised privacy concerns in relation to their mass deployment, particularly at large airports, including the revealing of individuals' naked bodies and medical conditions and the protection of individuals' data and images. These concerns largely align with Clarke's understanding of bodily privacy, privacy of behaviour and action and privacy of personal data. However, these scanners generate images that we regard as part of personal data.

Bodily 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".[33] The issue of "naked images" has also raised questions surrounding child protection laws, and the Electronic Privacy Information Center (EPIC) has argued that the capacity for viewing, storage and recall of images of children may contravene child protection laws.[34] According to privacy advocates, the images also show details of medical conditions that may be embarrassing for individuals. In 2002, the American Civil Liberties Union (ACLU) asserted that "passengers expect privacy underneath their clothing and should not be required to display highly personal details of their bodies…as a pre-requisite to boarding a plane".[35] 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.[36]

---

[31] Silvia Venier, "Global Mobility and Security," *Biometric Technology Today* 5 (2009).
[32] 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 February 2009.
[33] Demetrius Klitou, "Backscatter body scanners – A strip search by other means," *Computer Law & Security Report* 24 (2008): 317.
[34] Electronic Privacy Information Center, "Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding," Last modified June 2005, http://epic.org/privacy/surveillance/spotlight/0605/.
[35] American Civil Liberties Union, "The ACLU's view on body scanners", Last modified 15 March 2002, http://www.aclu.org/technology-and-liberty/body-scanners.
[36] Department for Transport, *Impact Assessment on the use of security scanners at UK airports*, Last modified Mar 29 2001. http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/consultations/open/2010-23/.

Images generated from body scanners could also reveal information about behaviour such as augmentation surgeries or medical related practices. For example, the ACLU has argued that body scanners reveal medical or lifestyle behaviour such as evidence of mastectomies, colostomy appliances, penile implants and/or catheter tubes, and thus provide details about individual behaviour. In terms of body imaging scanners, the issues related to privacy of behaviour and action significantly overlap with bodily privacy, however, the two are separate in the sense that it is the activities revealed by the images which individuals wish to conceal rather than the bodies or images themselves.

Concerns around data protection and data privacy 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.[37] 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.[38] EPIC argues that the fact that this capability could be re-enabled represents a data protection risk to passengers.[39] EPIC further notes that the TSA does not have a stellar reputation for protecting passenger data.[40] 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".[41] 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.[42] However, despite the link between body imaging scanners and privacy of personal data, the body scanners example makes clear that Clarke's conception of personal data needs to be expanded to include images as personal data.[43] Thus, data protection laws control the unauthorised storage, transfer and disclosure of personal data, precisely the issues of concerns that are expressed in relation to the images produced by body imaging scanners.

4.2 RFID-ENABLED TRAVEL DOCUMENTS

RFID-enabled travel documents include travel cards, such as Oyster Cards in London, which integrate RFID technology with the use of mass transportation in urban areas and RFID-enabled passports, also called e-passports, which are currently being introduced in most countries. Such RFID-enabled travel documents raise privacy concerns within the categories

[37] Ki Mae Heussner, "Air Security: Could Technology Have Stopped Christmas Attack?," *ABC News*, 29 December 2009. http://abcnews.go.com/Technology/AheadoftheCurve/air-security-technology-stopped-xmas-attack/story?id=9436877.
[38] Kim Zetter, "Airport Scanners Can Store, Transmit Images," *Wired News*, 11 January 2010. http://www.wired.com/threatlevel/2010/01/airport-scanners/.
[39] Philip Rucker, "US airports say seeing is believing as passengers face body-scan drill," *Sydney Morning Herald,* 5 January 2010. http://www.smh.com.au/travel/travel-news/us-airports-say-seeing-is-believing-as-passengers-face-bodyscan-drill-20100104-lq6o.html.
[40] EPIC, "Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding".
[41] Privacy International, "PI statement on proposed deployments of body scanners in airports", Last modified 31 December 2009. https://www.privacyinternational.org/article/pi-statement-proposed-deployments-body-scanners-airports
[42] 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 February 2011, 4.
[43] Even if the images are anonymised, this would not legitimate the circulation of such images. Circulation of such images without the authorisation of the person whose image was captured would be either illegal or morally repugnant or both.

of privacy of behaviour and action, privacy of data and image and privacy of location and space.

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. Location, time and other information stored on databases can be combined, which police have used to check the whereabouts or movements of suspects' during criminal investigations.[44] Furthermore, aggregated information can provide details that enable travellers' routines to be inferred. This can also materialise into a mistaken identity threat in that the association between an individual and a tag can be spurious (e.g., if the travel card or passport is stolen or given to another person), but the initial association is difficult to break once it is made.[45]

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. In RFID-enabled travel cards, the unique identifier on the chip is linked with personal information (e.g., if a person pays for the card by credit card, London Underground will have a record of all your travels and travel times). In RFID-enabled passports, the personal information stored on the chip can also be compromised by being read directly and without authorisation from the chip. 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 and/or their citizenship. Although basic protection measures such as access codes and Faraday cages[46] are built into e-passports to prevent unauthorised reading, Gellert and Gutwirth argue that these measures do not provide adequate protection[47] and do not possess the desired long-term security needed for e-passport applications (their validity is estimated to a maximum of 10 years).[48] Systems that store personal data, including biometric data, in back-end databases may also be vulnerable to data protection threats such as hacking, unauthorised access or unauthorised disclosure. Some systems have attempted to protect individuals from this threat by separating personal information from the RFID chip in the e-passport.[49] However, the resulting databases which store the sensitive personal information could represent a vulnerability. Finally, the unauthorised *use* of personal information also represents a privacy threat. In terms of RFID-enabled travel cards, marketing staff can target individuals based on the personal data they are required to submit in an application form and companies could

[44] "Oyster data use rises in crime clampdown", *The Guardian*, 13 March 2006. http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation and Octopus Holdings Limited, "Customer Data Protection".

[45] Marc Langheinrich, "A survey of RFID privacy approaches," *Personal and Ubiquitous Computing* 13 (2009): 414.

[46] Faraday cages are a metallic shielding embedded in the passport cover and designed to protect it from electronic eavesdropping.

[47] Faraday cages do not prevent eavesdropping on legitimate conversations between readers and tags, and basic access codes could enable counterfeiting, since a forger could splice together a valid electronic signature with false identity information and biometric components.

[48] Raphael Gellert and Serge Gutwirth, "Privacy, data protection and policy issues in RFID enabled e-passports," in *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright, 25 November 2011.

[49] Marc van Lieshout, et al., *RFID Technologies: Emerging Issues, Challenges and Policy Options*, Office for Official Publications of the European Communities, Luxembourg, 2007, 197.

aggregate these pieces of information to construct sophisticated consumer profiles.[50] This is especially true if contactless travel cards are expanded for use as payment for other small items.

Privacy of location and space is another aspect of privacy that is potentially undermined by RFID-enabled travel documents. Both RFID-enabled travel cards and e-passports carry the potential for a location threat, whereby individuals' movements can be monitored based on the RFID signature of their documents. Langheinrich argues that once a tag is associated with a particular person, the presence of the tag implies a location disclosure.[51] 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. Travellers may also be vulnerable to hotlisting, which 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.[52] In consequence, 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. This generalised threat materialises into specific threats, such as stalking[53] or unauthorised location disclosures to spouses, or other individuals.[54] However, in most places, police or other authorities must obtain a search warrant or court order in order to be given access to the data.[55] Finally, the RFID signals in passports or travel cards may also be tracked, since most RFID tags are standardised and will broadcast their signal to any compatible reader. This means that an individual could read an RFID chip's unique identifier, store it and follow its signal as long as the RFID reader is within range of the RFID-embedded travel card.

4.3 UNMANNED AIRCRAFT SYSTEMS

Despite a slow increase in the introduction of UASs in civil applications, such as law enforcement, border patrol and other regulatory surveillance, the use of unmanned aircraft systems (UASs or drones) has generated relatively muted debate about privacy and data protection. 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. However, the lack of noise and relative invisibility of UASs mean that individuals do not know if they are being monitored and UAS surveillance may often occur covertly.[56] Our discussion demonstrates that UASs raise issues of privacy of behaviour and action, privacy of data and image, privacy of location and space and privacy of association.

---

[50] Lara Srivastava, "Radio frequency identification: ubiquity for humanity," *info* 9 (2007).
[51] Langheinrich, "RFID privacy approaches".
[52] A. Juels, D. Molnar and D. Wagner, "Security and Privacy Issues in E-passports," in *Proceedings of IEEE/Create-net SecureComm 2005*, (Los Angeles CA: IEEE Computer Society Press, 2005), 79.
[53] Organisation for Economic Co-operation and Development, "RFID Guidance and Reports", *OECD Digital Economy Papers* 152 (Paris: OECD publishing, 2008), 42.
[54] Steve Bloomfield, "How an Oyster Card can Ruin your Marriage," *The Independent on Sunday*, 19 February 2006. http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html
[55] Octopus Holdings Limited, "Customer Data Protection", 2009.
[56] Rachel L. Finn and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law and Security Review* 28:2 (2012).

With surveillance-oriented drones, everyone is monitored regardless of whether their activities warrant suspicion; therefore, all behaviours are monitored and recorded. This potential for negative impacts on privacy of behaviour and action is particularly significant since UAS surveillance is much less overt than CCTV or helicopter surveillance to which it has been compared. The potential to use surveillance covertly means that in order to protect themselves from the negative effects of intrusions, individuals must assume they are being surveilled at all times and attempt to adjust their behaviour accordingly. This could introduce anticipatory conformity (a "chilling effect") where individuals alter their behaviour because they believe they may be under surveillance.[57]

UAS surveillance potentially infringes upon privacy of data and image in that it can generate images of individuals, sometimes covertly. This means that data protection principles contained in the 1995 Data Protection Directive (as well as the proposed Data Protection Regulation[58]) such as transparency, consent and rights of access can be undermined, because individuals may not even realise that they are subject to UAS surveillance at any given moment. Therefore, potentially covert data capture also leaves individuals with a limited ability to exercise privacy by taking "measures to keep private those activities that they do not wish to expose to public view".[59] One particular group who could be disproportionately affected by deployments of UASs in civil air space are celebrities whom paparazzi or other media could target with drones.

UAS devices can infringe upon privacy of location and space in that they can be used to track people or undermine their expectations regarding the boundaries of personal space. These surveillance devices can capture images of a person or a vehicle in public space, thereby placing individuals in particular places at particular times or revealing their movements through public space if more than one image is captured. UASs may also reveal information about private spaces such as back yards or, when flying low, can even transmit images of activities captured within homes, offices or other apparently private spaces. Thus, individuals who assume that their activities are not being monitored because they occur within the home or within private property may find that this assumption is false. The fact that this surveillance can be covert makes the capture of this information particularly problematic.

UAS devices may impact upon privacy of association through their ability to monitor individuals and crowds, again, sometimes covertly. Unmanned aircraft systems can 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.

4.4 SECOND-GENERATION DNA SEQUENCING TECHNOLOGIES

[57] Paul McBride, "Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations," *Journal of Air Law and Commerce* 74 (2009): 659.
[58] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 2012.
[59] McBride, "Beyond Orwell", 661.

Second-generation DNA sequencing technologies refer to the routine sequencing of the whole genomes of individuals rather than just distinct parts of the genome. Second-generation DNA sequencing impacts on the privacy of the person through the collection of intimate information that can potentially reveal personal data that are classified as sensitive. DNA sequences can reveal sensitive information about an individual and may indicate specific human qualities such as sex, sexual orientation, ethnicity, physical and mental health and predispositions to certain behaviours.[60] These categories are often associated with social marginalisation and discrimination, and revealing these traits can have significant impacts in terms of privacy of data and image. If this data is routinely revealed, individuals could become vulnerable to the consequences of genetic testing or could be effectively forced to undergo genetic testing in order to obtain insurance, employment or access to other goods and services.[61] These consequences could affect the individuals as well as their family members, due to the heritability of genetic information. As a result, second-generation DNA sequencing can impact upon privacy of the person, privacy of data and image, privacy of location and space and privacy of association.

Second-generation DNA sequencing impacts on the privacy of the person through the collection of intimate information that can potentially reveal personal data that are classified as sensitive. Currently, some police forces, such as those in the UK, are able to use reasonable force to take a DNA sample from arrested individuals, and military personnel in the USA are only able to refuse to submit a DNA sample for serious religious reasons.[62] While in these cases the taking of DNA samples does not take place on the basis of a mutual consent, this may change in the near future. Setting up biobanks for biomedical research involves the recruitment of large population cohorts and whole genome DNA sequencing will likely become a routine diagnostic test method in some areas of health care (e.g., for prenatal diagnosis). These examples suggest that consent could gradually become undermined as mandatory volunteerism becomes more commonplace.[63]

Second-generation DNA sequencing technologies potentially infringe upon the privacy of a person's data or image. As highlighted above, the information generated by DNA sequencing can potentially reveal sensitive data that increases the potential for genetic discrimination by government, insurers, employers, schools, banks and others.[64] Furthermore, despite the assumption that genetic data in databases can be rendered anonymous, it is possible that individuals could be identified[65], with all of the associated consequences. Lunshof et al. identify several avenues through which individuals could be de-anonymised, including:

- Inferring phenotype from genotype by identifying information in DNA and RNA, for instance, stature, hair or iris colour, or skin colour, or ethnic group
- Any amount of DNA data in the public domain with a name allows for identification within any anonymised data set

[60] "DNA confidential", *Nature Biotechnology* 27 (2009): 777.
[61] Piret Kukk, Bärbel Hüsing and Michael Friedewald, "Privacy, data protection and policy issues in next generation DNA sequencing technologies," *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright, 25 November 2011.
[62] Dorothy Nelkin and Lori Andrews, "DNA identification and surveillance creep," *Sociology of Health & Illness* 21 (1999).
[63] Gary T. Marx, "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information—'Hey Buddy Can You Spare a DNA?'," in *Surveillance and Security: Technological Politics and Power in Everyday Life*, ed. T. Monahan (London: Routledge, 2006).
[64] Kukk et al., "Next-generation DNA sequencing".
[65] L. Curren, et al., "Identifiability, genomics and UK data protection law," *European Journal of Health Law* 17 (2010).

- Security breaches based on attacks on or thefts or loss of DNA data.[66]

As such, like many other emerging technologies, the link between individuals and a "data set" requires a significant amount of attention to data protection mechanisms in order to protect privacy.

Whole genome DNA sequencing can 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 a 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 sensitive. Although whole genome sequencing is an emerging technology still in the research domain, the recent advent of low copy number DNA techniques[67] have led to mistakes in the criminal justice system, including false positive matches that suggested an individual's presence in a particular location[68] and matches resulting from secondary transfers associated with contamination.[69]

Finally, second-generation whole genome sequencing potentially impacts upon privacy of association in negative ways. An individual's presence at a particular gathering 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, and profiling enables individuals within particular groups to be identified. 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. 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.[70]

4.5 HUMAN ENHANCEMENT

Human enhancement technologies include those which offer enhancement via pharmacological means, i.e., neuro-enhancing pharmaceuticals (neuro-enhancers), or technical means via brain-computer interfaces (BCIs)[71]. Neuro-enhancing pharmaceuticals are characterised by their biological and chemical effects, and pharmaceutical neuro-enhancement comprises not only illegal drugs (amphetamines or cocaine), but also prescription and over-the-counter drugs such as aspirin and prescription drugs such as antidepressants, methylphenidate (Ritalin) and Aspirin. However, prescription drugs such as Ritalin may be misused or intentionally used for other purposes than the prescribed ones. The two most important categorisations of BCIs, particularly in relation to their privacy

[66] J.E. Lunshof et al., "From genetic privacy to open consent," *Nature Reviews Genetics* 9 (2008).
[67] Wikipedia defines Low Copy Number (LCN) as a DNA profiling technique developed by the Forensic Science Service (FSS) and in use in some countries since 1999.
[68] Rebecca Fowler, "Coded Revelations: DNA the second revolution", *The Observer*, 27 April 2003.
[69] Alan Hall, "Woman serial killer was a just phantom, German police admit," *The Telegraph*, 26 March 2009. http://www.telegraph.co.uk/news/worldnews/europe/germany/5056339/Woman-serial-killer-was-a-just-phantom-German-police-admit.html.
[70] Dustin Hays and DNA Policy Centre, "DNA, Forensics, and the Law", Last modified 2008. http://www.dnapolicy.org/policy.issue.php?action=detail&issuebrief_id=42.
[71] Philip Schütz and Michael Friedewald, "Technologies for Human Enhancement and their impact on privacy," in *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright, 25 November 2011.

invasiveness, is their location (invasive vs. non-invasive) and whether they operate 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 enable the user to control other digital or mechanical devices without the actual need of any neuro-muscular movement. Electroencephalography (EEG) that measures the electrical impulses emitted by the brain is the most prevalent sensing technology, and applications such as the mental typewriter or brain-to-robot interfaces are currently primarily being developed for therapeutic purposes. However, such technology could become more prevalent since the gaming and entertainment industry has recently shown an interest in the "reading" of brain activity to control and manipulate applications.[72] These human enhancement technologies carry the potential to impact upon privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image and privacy of thoughts and feelings.

Human enhancement may violate privacy of the person, both through neuro-enhancing pharmaceuticals and brain-computer interfaces, when the method of enhancement implies the internalisation of substances or technologies and/or a potential loss of control. On the one hand, Schütz and Friedewald argue that pharmaceutical neuro-enhancers enable the prescribing authority to exercise control over the recipient, affecting his/her bodily privacy.[73] On the other hand, BCI technology is based on both human and machine learning processes, which means that it could be possible to manipulate the BCI user.[74] Thus, Schütz and Friedewald further argue that any gain in control through the use of BCIs could easily be offset by a potential for loss of control. This confronts the user with unintended and potentially devastating consequences, particularly if the individual is dependent on the BCI-linked technology. For example, Parkinson's patients using BCIs such as deep brain stimulation have been confronted with side effects that include a change in their personality.

Human enhancement technologies potentially impact upon privacy of behaviour and action in two ways. First, as mentioned above, neuro-enhancers are closely linked to the risk of losing control over one's will and actions. That is why prescribed "enhancing" drugs such as Ritalin or Modafinil pose a threat of external control over the individual's behaviour. Second, 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. In this context, individuals could be exposed to preventive strategies, such as crime prevention.[75] Furthermore, individuals could be influenced to buy certain products, or spend more money than they otherwise would, based on an interaction between mood, purchasing behaviour and external stimulation.[76]

Privacy of communication may be impacted by brain-computer interfaces, whereby the interception or monitoring of data streams between the BCI user and the machine could be possible. When BCIs are used to assist individuals in communicating with others, the data that passes between the user and the communication software could be intercepted and

[72] Anton Nijholt, "BCI for Games: A 'State of the Art' Survey", in *Entertainment Computing - ICEC 2008*, eds. Scott M. Stevens, and Shirley J. Saldamarco (Berlin: Springer, 2009), 225.
[73] Schütz and Friedewald, "Technologies for Human Enhancement and their impact on privacy".
[74] Dennis J. McFarland and Jonathan R. Wolpaw, "Brain-computer interfaces for communication and control," *Communications of the ACM* 54 (2011): 63.
[75] Adam Kepecs, "Neuroscience: My brain made me do it," *Nature* 473 (2011).
[76] Ira van Keulen and Mirjam Schuijff, "Engineering of The Brain: Neuromodulation and Regulation," in *Making Perfect Life: Bioengineering in the 21st Century*, eds. Rinie van Est and Dirk Stemerding (Brussels: European Technology Assessment Group, June 2011).

analysed. Furthermore, recent scientific research in brain imaging and speech has begun to identify electrical patterns associated with certain words or phrases.[77] As BCIs develop, more of the content of communication could become vulnerable to interception.

Privacy of data and image is only touched upon in relation to human enhancement technologies that are capable of collecting data, regardless of how it may be further processed. As such, BCIs are the only human enhancement technology that potentially impacts upon privacy of data and image because they involve the digitalisation, collection, (temporary) storage and processing of information about brain activity. This data is highly sensitive, because the prospective worth of such unique personal information may increase exponentially in terms of its marketing value for the advertisement industry. In addition, it is difficult to anticipate what information can be collected and/or extracted in the future and whether it will be financially lucrative. Despite this, Schütz and Friedewald note that system security was given little thought when researchers first developed the technical infrastructure of BCIs, as was the case in the early days of the Internet. Thus, BCI technologies are vulnerable to breaches through hacking or other intrusions.[78] However, at the moment, this threat is relatively inconsequential as current BCIs are not designed to extract data, they merely link individuals with other assistive technologies.

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. According to McFarland and Wolpaw, the images created by the brain's electrical impulses reveal 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."[79] Such technologies are being explored in relation to counter-terrorism and advertising practices, where, for example, sensor networks are being deployed in semi-public spaces to detect stress levels to attempt to identify suspicious behaviour and are being developed for retail situations to attempt to predict and influence purchasing behaviour. In the counter-terrorism context, such data could lead to additional questioning or refusal of services, which would impact upon a person's privacy of thoughts or feelings. Shoppers could also be influenced in the retail sector or targeted based on the feelings that they present, leading to discrimination or other profiling practices. In either context, such technology could encourage individuals to attempt to conceal thoughts or feelings in anticipation of such measurements since their thoughts or feelings could become public information.

4.6 SECOND-GENERATION BIOMETRICS

In parallel with their wider deployment, biometrics have raised critical privacy and data protection issues which have impacted the acceptability of biometric identification methods. The next generation of biometrics include the measurement and analysis of new biometric traits, such as behavioural or soft biometrics (i.e., biometrics which may change over time, such as gait analysis and voice recognition software) and physiological biometrics (including heartbeat detection, pheromone detection). In second-generation biometrics, these soft or

[77] Ian Sample, "Mind-reading program translates brain activity into words," *The Guardian*, 31 January 2012. http://www.guardian.co.uk/science/2012/jan/31/mind-reading-program-brain-words

[78] Medical Device Security Center, "Medical Device Security Center", Last modified 2011. http://secure-medicine.org/.

[79] Martha J. Farah, "Neuroethics: The practical and the philosophical," *Trends in Cognitive Sciences* 9 (2005): 34.

physiological traits are often used in combination with more traditional traits in *multiple biometrics* or *multimodal systems* to strengthen identification systems. Venier and Mordini argue 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.[80] However, many of the applications of second-generation biometrics are still in the research domain and second-generation biometrics are most appropriately classed as emerging technologies. Unique to other technologies discussed here, second-generation biometrics affects all of the seven types of privacy we outline in this article. Some soft biometrics such as the way one walks (gait) or types a letter could be regarded as unconscious behaviour. However, we would regard these as still different from privacy of behaviour and action as these possibly supposed unconscious behaviours reflect a personal characteristic (privacy of the body) rather than the intentionality that is implicit in privacy of behaviour and action.

In relation to second-generation biometrics, privacy of the person could be impacted by the systematic collection of information that could be used for classification purposes. Venier and Mordini argue that second-generation biometrics potentially infringe upon human dignity through the measurement and digitalisation of the body.[81] 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. Because of the potential for classification, Venier and Mordini are concerned that 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.[82] This could be exacerbated as more, sometimes superfluous, data is collected by multiple biometrics and multimodal systems, in order to improve system performance. Furthermore, the collection of biometric information remotely, covertly and/or at a distance could mean that individuals' bodies are routinely measured and mined for information without the explicit consent of the person who is being monitored.

Soft biometrics potentially impact privacy of behaviour and action through processes of automation. According to Venier and Mordini, 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 can also become automated which could lead to monitoring and recording of infrequent behaviours that are not suspicious or criminally deviant. Physiological 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, as a result of pre-emptive discriminatory measures.

Soft biometrics, specifically voice or speech recognition technologies, can negatively impact individuals' privacy of personal communications. Speech or voice recognition technologies can be utilised to record, analyse and disclose the content of communication. Although these are not the primary purpose of such technologies, the infrastructure necessary to record and verify human voices or human speech can be relatively easily re-worked to enable such

[80] Silvia Venier and Emilio Mordini, "Second-generation biometrics", in *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright, 25 November 2011.
[81] Venier and Mordini, "Second-generation biometrics".
[82] Ibid.

recording and disclosure of the content of speech. Such re-oriented voice or speech recognition technologies can also be linked with automated systems to ensure that communications by certain individuals, or communications about certain topics, can be monitored or recorded. This could discourage individuals who use certain types of voice recognition systems from communicating with particular people or about particular topics in areas where voice recognition systems are in operation.

Soft biometrics and the use of biometrics at a distance both pose a threat to personal data and image. Article 33 of the proposed new Data Protection Regulation says that the processing of biometric data presents specific risks, meaning that it must be processed in respect of principles such as consent and proportionality. Some types of soft biometrics, and especially biometrics at a distance, can present a risk that an individual would not know that a system was in operation and thus would not have consented to the collection of their biometric information and may not be able to exercise their rights to access that data. Behavioural biometrics also 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. Finally, the fact that soft biometrics often collect additional, unnecessary information raises issues surrounding the principle of proportionality.

Physiological biometrics can impact privacy of thoughts and feelings through the collection of intimate information that can be used to detect suspicious behaviour or predict intention or susceptibility. Imaging scanners that combine physiological measurements intended to detect heightened emotional states could provide clues to an individual's state of mind and potentially lead to discrimination.[83] 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. Examples of such applications include counter-terrorism applications as well as personalised advertising applications where individuals' experience of semi-public space is restricted or impacted by the emotional state "read" by biometric sensors. Again, the danger is not necessarily that the individual is identified, but that they are categorised and decisions are made about them based on the profile they present.

Second-generation biometrics such as embedded systems and soft biometrics may also negatively impact privacy of location and space. Unlike current-generation overt biometric systems used to authenticate or identify an individual with their co-operation, sensing and identifying individuals at a distance can result in covert data capture without the data subject's consent. This means that a biometric system can create a link between an individual and a location at a particular time without their co-operation, and without their being aware that this occurred. Thus, there is a clear overlap with the privacy concerns associated with privacy of the person. Individuals could also be tracked without being identified by using biometrics to differentiate a particular person as they move through public space. 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.

Finally, soft biometrics may negatively impact privacy of association. Soft biometrics introduces concerns that individual members of a group could be identified at a distance through the linking of such biometrics to other data sets. Furthermore, behavioural analysis

[83] "Where Decisionmaking Is Measured", *Harvard Magazine*, 12 December 2008. http://harvardmagazine.com/breaking-news/where-decisionmaking-is-measured

could be used to identify leaders or vulnerable members of a group, enabling group organisation and decision making structures to be revealed.

4.7 FILLING IN THE GAPS

Despite the utility of Clarke's four categories of privacy, particularly in relation to the identification of specific types of privacy which must be protected, our case studies reveal that new and emerging technologies introduce new and additional types of privacy that Clarke did not consider in his original piece. Our conceptualisation maintains two of Clarke's original categories: privacy of the person and privacy of personal communication.[84] We have also re-worked Clarke's categories of privacy of personal behaviour and privacy of personal data to privacy of behaviour and action and privacy of data and image respectively. The change to privacy of behaviour *and action* is because we regard behaviour and action as both characterised by intentionality, but "action" is slightly different from "behaviour". Action has an element of planning that is not normally present in behaviour. We would not want to overstate this, however. One can act (behave) in a certain way in response to a certain stimulus (if someone slaps you in the face, you might slap back, and there probably is precious little time to "plan" such a response), but on the other hand, if you are an assassin, you probably have a fair amount of time to plan your next hit (action). The change to privacy of data and image is intended to highlight the image as a form of personal data that increasingly can be mined for biometric data and used to identify, monitor and/or track individuals as they move about public or semi-public space.

Furthermore, three additional aspects of privacy were necessary to fully capture the privacy impacts of the new and emerging technologies that we discussed here. Clarke's original framework did not include privacy of location and space, privacy of thoughts and feelings and privacy of association (including group privacy). Although Clarke includes some consideration of "space" within his category of privacy of behaviour, our understanding of location and space includes the potential to connect an individual to a particular location at a particular time, rather than simply monitoring that person as they move about in particular spaces. Furthermore, privacy of location and space includes the possibility that the individual moving about space can be connected to a digital persona, or that location information could be aggregated to actively or retrospectively track an identifiable individual as they move around in public or semi-public space (e.g., shopping malls) or private property (e.g., stores, office buildings). In addition to RFID-enabled travel documents, and the other examples discussed in this paper, automatic number plate recognition (ANPR) systems, CCTV cameras fitted with facial recognition and global positioning system surveillance such as chips carried in smart phones also perform similar functions with similar associated potential privacy impacts.

The inclusion of privacy of thoughts and feelings addresses another gap in Clarke's categorisation. Emerging technologies such as brain computer interfaces, as well as neuro-imaging, neural modulation and biometric sensor arrays (heart rate monitors, skin temperature sensors, pupil dilation) all have the possibility to disrupt the interiority of the body and mind to provide clues about thoughts, feelings and/or states of mind. This differs from privacy of the person in that privacy of the person focuses on identifying, reflecting and classifying the physical body, whereas privacy of thoughts and feelings targets the more

[84] As mentioned early on in this article, Clarke labelled privacy of personal data and privacy of personal communications as "information privacy".

ephemeral aspects of the person. Furthermore, privacy of thoughts and feelings protects what is perhaps the least controversial, most consistent and unwavering dimension of privacy, the individual thoughts and feelings which until now were almost entirely imperceptible to others unless individuals chose to share them.

Finally, privacy of association connects privacy, as a heterogeneous but largely individualised concept, to interpersonal relationships. As recognised by Article 8 of the Charter of Fundamental Rights, privacy includes respect for both individual and family life, thus inter-personal relationships form part of the European conception of privacy. Second, privacy of association links directly with other fundamental rights such as rights to assembly, religious freedom and free speech. New and emerging technologies enable individuals and their inter-relationships to be revealed through DNA sequencing technology that identifies family relationships or enables individuals to be organised into groups based on physical traits, technologies such as UAS surveillance or second-generation biometrics which can link identifiable individuals to particular places at particular times and behavioural analytic technologies which can analyse behaviour to better understand relationships between group members and/or group structures. These additional aspects of privacy are most visible in relation to new and emerging technologies and have expanded our understanding of different types of privacy. The next section will examine how the heterogeneity and flexibility of privacy, as a concept, needs to be maintained in order to continue to address the potential impacts associated with technological developments.

5 THE MERIT OF ELUSIVENESS

As mentioned above, Gutwirth refers to a definition of privacy as "elusive". In this summary section, we argue that privacy is an inherently heterogeneous, fluid and multidimensional concept, and we suggest that this multidimensionality may be necessary to provide a platform from which the effects of new technologies can be evaluated. This potential necessity is supported by the fact that different technologies impact upon different types of privacy, and further technological changes may introduce or foreground previously unconsidered privacy dimensions.

Our case study discussion above demonstrates that different technologies potentially impact upon different types of privacy and embody different risks to privacy. Table 1, below, summarises the spread of privacy types that new and emerging technologies may impact upon. 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. Therefore, scholars, legal theorists, policy makers and other actors must maintain an awareness that there are different types of privacy in order to ensure adequate protection of individuals (and society) in relation to existing and emerging technologies, applications and practices.[85]

[85] We do not mean to suggest that the newer the technology, the broader the risks to these different dimensions of privacy. Each new technology must be assessed to determine whether it has impacts on privacy and, if so, which types of privacy. It does not follow that new technologies necessarily pose greater risks to privacy than older technologies, but it is certainly true, as we have demonstrated, that some new technologies have exposed types of privacy not heretofore considered and that as technologies become more complex, the more likely it is that the risks will also be more complex.

This also means that the protection of data that *describes* a person will remain important in the future. However, with the advent of new technologies such as next-generation biometrics, DNA sequencing and human enhancement technologies the data being collected moves from simply describing a person to being an *inherent part* of the person. This calls for a much stronger focus on an ethical assessment element to complement established (and enhanced) data protection principles.

Technology / Type of privacy	Whole body imaging scanners	RFID-enabled travel documents	Unmanned aircraft systems	Second-generation DNA sequencing	Human enhancement technologies	Second-generation biometrics
Privacy of the person	X			X	X	X
Privacy of behaviour and action	X	X	X	X	X	X
Privacy of communication					X	X
Privacy of data and image	X	X	X	X	X	X
Privacy of thought and feelings					X	X
Privacy of location and space		X	X	X		X
Privacy of association			X	X		X

Table 1: Aspects of privacy potentially impacted by case study technologies

We also suggest that the fluidity of privacy as a concept may be an important aspect of its utility, since technological developments may introduce new types of privacy. As technologies develop and proliferate, various types of privacy which had not previously been considered or identified as under threat may become compromised. While the privacy experts quoted in section 2 lament the fact that privacy is difficult to define and conceptualise, we propose that fluidity and flexibility are necessary to enable "privacy" to respond to technological changes. More precise conceptualisations, taxonomies and boundaries surrounding privacy, particularly in the legal field, may disrupt the use of privacy to protect individuals and groups from intrusions that impact upon their freedoms, fundamental rights and access to goods and services.[86] Therefore, despite other theorists' frustration with the difficulty in defining privacy, perhaps maintaining its elusiveness carries particular benefits for law-makers and citizens. In any event, we believe that our typology offers benefits, as we stated earlier, for policy-makers, academics, privacy advocates and any organisation carrying out a reasonably comprehensive privacy impact assessment.

[86] We draw support in this conclusion from Gutwirth, *Privacy and the information age,* pp. 33-34, who discusses the undesirability of defining privacy from a legal perspective.

6 CONCLUSION

This paper has provided three main theoretical arguments. First, we have demonstrated that privacy is a fluid and dynamic concept that has developed alongside technological and social changes. In the 15 years between 1997 and 2012, the advent of new technologies and applications has meant that previously unconsidered types of privacy now need to be addressed in order to adequately protect individuals' rights, freedoms and access to goods and services. Second, we have identified seven different types of privacy that current decision-makers need to consider in providing proactive protection to individuals in the face of new and emerging technologies. These include privacy of the person, privacy of behaviour and action, privacy of data and image, privacy of communication, privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy). Each of the different technologies discussed here impact upon different types of privacy and all of these types need to be considered when formulating privacy protections.[87] Third, we have proposed that one of the strengths of privacy is its complexity, fluidity and heterogeneity. Decision-makers, and most especially policy-makers, may find benefit in maintaining a fluid and mutable understanding of privacy in order to ensure that privacy is protected in the face of future technological developments.

[87] Privacy should not be narrowly defined, nor should information privacy (of communication and personal data protection) be regarded as all there is to privacy. Clarke speaks of a "serious debasement of the term 'privacy' [which] has occurred in the case of U.S. and Australian statutes that have equated it with the highly restrictive idea of 'data protection'. That notion derives from the 'fair information practices' movement that has been used by corporations and governments since the late 1960s to avoid meaningful regulation." Roger Clarke, "What's 'privacy'?", Xamax Consultancy, 2006. http://www.rogerclarke.com/DV/Privacy.html

7 REFERENCES

American Civil Liberties Union. “The ACLU's view on body scanners.” Last modified 15 March 2002. http://www.aclu.org/technology-and-liberty/body-scanners

Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca NY: Cornell University Press, 1992.

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

Clarke, Roger. “Introduction to Dataveillance and Information Privacy, and Definitions of Terms” (Xamax Consultancy, Aug 1997). http://www.rogerclarke.com/DV/Intro.html

Clarke, Roger. “What’s ‘Privacy’?” *Australian Law Reform Commission Workshop*. 28 July 2006. http://www.rogerclarke.com/DV/Privacy.html

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* 17 (2010): 329-344.

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/

“DNA confidential.” *Nature Biotechnology* 27 (2009): 777.

Electronic Privacy Information Center (EPIC). “Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding.” Last modified June 2005.
http://epic.org/privacy/surveillance/spotlight/0605

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 February 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 February 2011.

Farah, Martha J. “Neuroethics: The practical and the philosophical.” *Trends in Cognitive Sciences* 9 (2005): 34-40.

Finn, Rachel L., and David Wright. “Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications.” *Computer Law and Security Review* 28:2 (2012) [forthcoming].

Fowler, Rebecca. “Coded Revelations: DNA the second revolution.” *The Observer*, 27 April 2003.

Fuchs, Christian. “Towards An Alternative concept of privacy.” *Journal of Information, Communication and Ethics in Society* 9 (2011): 220-237.

Gellert, Raphael and Serge Gutwirth. “Privacy, data protection and policy issues in RFID enabled e-passports.” In *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* PRESCIENT Deliverable 2, edited by Rachel Finn and David Wright, 31-59. 25 November 2011.

Goold, Benjamin J. “Surveillance and the Political Value of Privacy.” *Amsterdam Law Forum* 1 (2009): 3-6.

Gutwirth, Serge. *Privacy and the information age*. Lanham, MD: Rowman & Littlefield, 2002.

Hall, Alan. “Woman serial killer was a just phantom, German police admit.” *The Telegraph*, 26 March 2009.
http://www.telegraph.co.uk/news/worldnews/europe/germany/5056339/Woman-serial-killer-was-a-just-phantom-German-police-admit.html

Hays, Dustin, and DNA Policy Centre. “DNA, Forensics, and the Law”. Last modified 2008.
http://www.dnapolicy.org/policy.issue.php?action=detail&issuebrief_id=42

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

Juels, A., D. Molnar, and D. Wagner. "Security and Privacy Issues in E-passports." In *Proceedings of IEEE/Create-net SecureComm 2005*, 74-88. Los Angeles CA: IEEE Computer Society Press, 2005.

Kaspar, Debbie V.S. “The Evolution (or Devolution) of Privacy.” *Sociological Forum* 20 (2005): 69-92.

Kepecs, Adam. “Neuroscience: My brain made me do it.” *Nature* 473 (2011): 280-281. Accessed 2 March 2012. http://www.nature.com/doifinder/10.1038/473280a

Klitou, Demetrius. “Backscatter body scanners – A strip search by other means.” *Computer Law & Security Report* 24 (2008): 316-325.

Kukk, Piret, Bärbel Hüsing and Michael Friedewald. “Privacy, data protection and policy issues innext generation DNA sequencing technologies.” In *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* PRESCIENT Deliverable 2, edited by Rachel Finn and David Wright, 143-174. 25 November 2011.

Langheinrich, Marc. “A survey of RFID privacy approaches.” *Personal and Ubiquitous Computing* 13 (2009): 413-421.

Lunshof, J.E., R. Chadwick, D.B. Vorhaus and G.M. Church. “From genetic privacy to open consent.” *Nature Reviews Genetics* 9 (2008): 406-411.

Lyon, David. *Surveillance after September 11*. Cambridge: Polity Press, 2003.

McBride, Paul. “Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations.” *Journal of Air Law and Commerce* 74 (2009): 627-662.

McFarland, Dennis J., and Jonathan R. Wolpaw. “Brain-computer interfaces for communication and control.” *Communications of the ACM* 54 (2011): 60-66.

MacKinnon, Catharine A. *Feminism Unmodified: Discourses on Life and Law*. Cambridge, MA: Harvard University Press, 1987.

Marx, Gary T. “Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information—‘Hey Buddy Can You Spare a DNA?’” In *Surveillance and Security: Technological Politics and Power in Everyday Life,* edited by Torin Monahan, 37-56. London: Routledge, 2006.

Marx, Gary T. “Privacy is not quite like the weather” in *Privacy Impact Assessment*, edited by David Wright and Paul De Hert. Dordrecht: Springer, 2012.

Medical Device Security Center, “Medical Device Security Center”, 2011. http://secure-medicine.org/

Emilio Mordini, “Whole Body Imaging at airport checkpoints: the ethical and political context.” In *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, edited by René von Schomberg, 165-209. Luxembourg: Publications Office of the European Union, 2011.

Nelkin, Dorothy, and Lori Andrews. “DNA identification and surveillance creep.” *Sociology of Health & Illness* 21 (1999): 689–706.

Nijholt, Anton. “BCI for Games: A 'State of the Art' Survey.” In *Entertainment Computing - ICEC 2008*, edited by Scott M. Stevens and Shirley J. Saldamarco, 225-228. Berlin: Springer, 2009.

Nissenbaum, Helen “Privacy as Contextual Integrity”, *Washington Law Review,* 79:1 (2004): 101-139.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford CA: Stanford University Press, 2010.

Octopus Holdings Limited. “Customer Data Protection”. Last updated 2009.

Organisation for Economic Co-operation and Development. “RFID Guidance and Reports.” *OECD Digital Economy Papers* 152, Paris: OECD publishing, 2008.

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

Privacy International. “PI statement on proposed deployments of body scanners in airports.” Last updated 31 Dec 2009. https://www.privacyinternational.org/article/pi-statement-proposed-deployments-body-scanners-airports

Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy, (*Chapel Hill, University of North Carolina Press, 1995): 220-231;

Rucker, Philip. “US airports say seeing is believing as passengers face body-scan drill.” *Sydney Morning Herald,* 5 January 2010. http://www.smh.com.au/travel/travel-news/us-airports-say-seeing-is-believing-as-passengers-face-bodyscan-drill-20100104-lq6o.html

Sample, Ian. “Mind-reading program translates brain activity into words.” *The Guardian*, 31 January 2012. http://www.guardian.co.uk/science/2012/jan/31/mind-reading-program-brain-words

Schütz, Philip and Michael Friedewald. “Technologies for Human Enhancement and their impact on privacy”, In *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* PRESCIENT Deliverable 2, edited by Rachel Finn and David Wright, 175-198. 25 November 2011.

Solove, Daniel J. *Understanding Privacy*. Cambridge MA: Harvard University Press, 2008.

Solve, Daniel. “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.” *San Diego Law Review* 44 (2007): 745- 772.

Srivastava, Lara. “Radio frequency identification: ubiquity for humanity.” *Info* 9 (2007): 4-14.

Steeves, Valerie. “Reclaiming the social value of privacy”, in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* edited by Ian Kerr, Valerie Steeves and Carole Lucock, (Oxford University Press, 2009).

Supreme Court of Canada, R. v. Dyment (188), 55 D.L.R. (4th) 503 at 513 (S.C.C.).

van Keulen, Ira, and Mirjam Schuijff. “Engineering of The Brain: Neuromodulation and Regulation.” In *Making Perfect Life: Bioengineering in the 21st Century*, edited by Rinie van Est and Dirk Stemerding, 68-116. European Technology Assessment Group, June 2011.

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*. Luxembourg: Office for Official Publications of the European Communities, 2007.

Venier, Silvia and Emilio Mordini. “Second-generation biometrics”, In *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* PRESCIENT Deliverable 2, edited by Rachel Finn and David Wright, 111-142. November 25 2011.

Venier, Silvia. “Global Mobility and Security.” *Biometric Technology Today* 5 (2010): 7-10.

Warren, Samuel and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review* 4, (1890): 193-220.

Westin, Alan. “Social and Political Dimensions of Privacy,” *Journal of Social Issues*, 59: 2 (2003): 431-453.

“Where Decisionmaking Is Measured”, *Harvard Magazine*, Dec 12 2008. http://harvardmagazine.com/breaking-news/where-decisionmaking-is-measured

Whitman, James Q. “The Two Western Cultures of Privacy: Dignity Versus Liberty.” *The Yale Law Journal* 113 (2004); 1151-1221.

Zetter, Kim. “Airport Scanners Can Store, Transmit Images.” *Wired News*, January 11 2010. http://www.wired.com/threatlevel/2010/01/airport-scanners/