Privacy principles, risks and harms

Cite As: Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. International Review of Law, Computers and Technology, 28(3), 277-298. 10.1080/13600869.2014.913874

Privacy principles, risks and harms

Abstract

The protection of privacy is predicated on the individual's right to privacy and stipulates a number of principles that are primarily focused on information privacy or data protection and, as such, are insufficient to apply to other types of privacy and to the protection of other entities beyond the individual. This article identifies additional privacy principles that would apply to other types of privacy and would enhance the consideration of risks or harms to the individual, to groups and to society as a whole if they are violated. They also relate to the way privacy impact assessment (PIA) may be conducted. There are important reasons for generating consideration of and debate about these principles. First, they help to recalibrate a focus in Europe on data protection to the relative neglect of other types of privacy. Second, it is of critical importance at a time when PIA (renamed 'data protection impact assessment', or DPIA) may become mandatory under the European Commission's proposed Data Protection Regulation. Such assessment is an important instrument for identifying and mitigating privacy risks, but should address all types of privacy. Third, one can construct an indicative table identifying harms or risks to these additional privacy principles, which can serve as an important tool or instrument for a broader PIA to address other types of privacy.

Keywords: privacy principles; types of privacy; privacy risks; privacy impact assessment; surveillance impact assessment

Introduction

The protection of information privacy has made significant advances during the past 40 or 50 years, with the global proliferation of national, sub-national and international legislation, the development of rights-based jurisprudence, and a plethora of regulatory initiatives and practical measures to safeguard 'personal data' or 'personally identifiable information' (PII) (Bennett and Raab 2006). These developments have been predicated upon sets of privacy principles that can be used to identify problematic practices in the processing of such information. Regulatory measures have emphasised the necessity of mitigating threats to individuals posed by the burgeoning appetite, in both the public and private sectors, for collecting, using and sharing data for a host of commercial and governmental purposes.

There have been many formulations of privacy principles since the 1960s and 1970s, when the main concern of policy-makers and commentators was with 'computers-and- privacy' issues generated by 'data banks' and their use. These codifications have therefore primarily focused on only one type of privacy, i.e., information privacy or data protection, even though – as we will show – several other types of privacy also have claims to protection. However, there have been no formulations of privacy principles that specifically address these other types of privacy, nor of the privacy risks or harms that could arise from their violation.

While the link between privacy and human rights is widely acknowledged, historically rooted, and strong, modern developments in the 'information age' have brought the information and communication dimensions to the fore and equipped them with regulatory instruments for their protection. It is not clear how far other types of privacy can be, or are, subsumed or incorporated into the theory and practice of information privacy protection, but they are too important to be left in the background or implicit in the protections afforded to 'privacy' by national or international law and regulation that focus specifically on the processing and flows of personal information. As we show, regulatory practitioners in several countries have moved towards recognising the invasion of other types of privacy besides information privacy as requiring regulation. However, now that there is a heightened perception and deeper understanding of the pervasiveness of surveillance, as well as recognition of its effects beyond that of individual privacy, there is a need to move towards a formulation of principles for mitigating these effects beyond the compass of information privacy principles and their implementation.

Bennett (2011) has argued that information privacy protection has, in practice, already widened its horizon to include social effects and implications for other dimensions of privacy besides the informational. The current article acknowledges the force of this defence and aims to take its message seriously by grounding more systematically the widening of the inventory of norms and instruments for a broader protection of privacy. It is not that 'privacy' is too narrow or impotent to contend with contemporary infringements of rights, but that information privacy and the array of principles designed specifically for its protection might be too limited for this contention. It has been remarked that information privacy principles 'are oriented towards the protection of data about people, rather than the protection of people themselves' (Clarke 2000, s. 2.4). Can a further step be taken, towards a fuller view of

people's privacy and how it can be protected? This article proposes a more comprehensive view of privacy and the principles that might be devised for its better and more holistic protection.

The present article supports a broader protection of privacy by positing a set of privacy principles that can support privacy rights other than data protection. We also favour an innovation in privacy impact assessment (PIA), i.e., a PIA that specifically addresses types of privacy other than, or in addition to, data protection. As will be shown later (Table 2), examples of the harms and risks that can arise in regard to other types of privacy can be enlisted in support of the PIA innovation proposed here.

This article reviews various formulations of information privacy principles that have shaped regulatory practice over a long period of time. It then refers to an expanded inventory of seven types of privacy and goes on to identify additional privacy principles that pertain to them. Following a discussion of privacy risks, the article concludes with arguments that show why privacy principles need to be debated. Although case law in Europe and the USA shows that the courts have pronounced on a wider variety of types of privacy, legal analysis is outside the scope of this paper. We argue that there is a need to recalibrate privacy and data protection policy and regulation by extending their scope.

Approach and methodology

We address our topic by taking, broadly speaking, the following main steps: First, we identify the problem – i.e., there is a great risk of equating privacy and data protection. Data protection is only one type of privacy, and there are several types of privacy, all of which merit protection. However, in Europe, data protection gets more attention from policy-makers than other types of privacy.

Second, we sketch the argument on which this article turns. We argue that other types of privacy are important and must be acknowledged, otherwise we risk greatly circumscribing the notion of privacy.

Third, we note that data protection is supported by various principles, and that the other types of privacy should also be served by a set of principles. We define privacy principles and rights.

Fourth, privacy principles are important because they form the basis for the formulation of questions that organisations can use to determine whether their new technology, system, project or policy might pose risks to one or more types of privacy. We give some examples of risks to other types of privacy.

Fifth, we argue that PIA provides a good framework for identifying, assessing and managing privacy risks. However, PIA can be distinguished from DPIA. The process for undertaking each is virtually identical, but their scopes are different.

Sixth, we draw some conclusions and identify some solutions to the challenges identified in this article.

En route to our conclusions, we present two tables, the first of which shows a correlation between specific privacy principles and types of privacy, while the second provides an indicative list of the privacy principles articulated in this article and the types of harms or risks that could violate these principles. As noted elsewhere, such tables may be useful in PIA and surveillance impact assessment (SIA).

The methodology used for preparing this article primarily consists of desk research and reasoned argument. It does not include surveys, interviews or other techniques for gathering empirical data.

Privacy principles

The principles on which regulatory systems for information privacy have been built give rise to rules and guidelines for the fair collection and processing of personal data, although legal and practical experience over many years has shown that 'personal data' is not an unambiguous concept. Regulatory law and practice ideally depend upon precision in the expression and elaboration of principles and the guidelines, codes of practice and other instruments that constitute implementation. Given the globalisation of information processing, consistency in the enunciation of principles and perforce in their legal embodiment and practical interpretation has been seen as important, although concrete variations are tolerable as long as the underlying principles are reasonably uniform.

However, a broad brush is useful at this stage of the argument. Generally speaking, while the numbering and wording of the principles vary in different formulations, a consen- sus exists. Thus, to paraphrase legal language, a public or private organisation that deals with PII should: be accountable for all of the personal information in its possession; identify the purposes for which the information is processed at or before the time of collection; only collect personal information with the knowledge and consent of the individual (except under specified circumstances); limit the collection of personal information to that which is necessary for pursuing the identified purposes; not use or disclose personal information for purposes other than those identified (except with the individual's consent); retain information only as long as necessary; ensure that personal information is kept accurate, complete and up to date; protect personal information with appropriate security safeguards; be transparent about its policies and practices and maintain no secret information system; allow data subjects access to their personal information, with an ability to amend it if it is inaccurate, incomplete or obsolete (Bennett and Grant 1999, 6).

For analysing wider realms of privacy beyond information privacy, and for exploring harms or risks, it is useful to go beyond pastiche and look at the provenance and more recent adoption, in selected jurisdictions, of what are taken to be the principles as distilled into colloquial or summary expressions. These strictures are manifested in some of the most influential documents from the 1970s to the present, illustrating the predominance of information privacy and its principles in regulatory development.[1] An early enunciation of information privacy principles was in the US Department of Health Education and Welfare (HEW)'s 1973 Fair Information Practice Principles ('FIPPs') (HEW 1973).[2] The

Organisation for Economic Co-operation and Development (OECD 1980) drew on these but expanded them.[3] They cover collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability. The OECD Guidelines have been very influential across the world in countries' adoption of their own data protection legislation. They explicitly state that they apply only to personal data:

> the Guidelines do not constitute a set of general privacy protection principles; invasions of privacy by, for instance, candid photography, physical maltreatment, or defamation are outside their scope unless such acts are in one way or another associated with the handling of personal data.[4]

Thus, the OECD implicitly recognises other types of privacy and the need for privacy principles beyond its own. In 2005, the Asia-Pacific Economic Cooperation's Privacy Framework (APEC 2005) adopted nine 'information privacy principles', which built upon the OECD Guidelines and sought to modernise them (Cate 2006, 353).

The Council of Europe's 1981 Convention (CoE 1981) has had a greater influence than the OECD Guidelines in the legislation of European Union (EU) Member States and in the EU's own data protection Directive 95/46/EC (European Parliament and the Council 1995) (to be superseded by a new Regulation). With minor, albeit important, changes of wording, the Directive replicated these Convention Articles, and added further rules about the legitimacy of processing and the transfer of personal data to third countries.[5]

Other sets of principles can be found.[6] Australia's Privacy Amendment (Enhancing Privacy Protection) Act 2012 came into force from March 2014. The new Act contains significant reforms to the Privacy Act, including replacing the National Privacy Principles for the private sector and Information Privacy Principles for Commonwealth and Australian Capital Territory Government agencies with a single consolidated set of principles referred to as the Australian Privacy Principles ('APPs').[7] The Canadian Standards Association (1996) has a set of 10 principles based on the OECD Guidelines. New Zealand's Privacy Act 1993 sets out 12 information privacy principles (IPPs), based upon international principles of fair information practice.[8]

In December 2011, the International Organization for Standardization published an international standard for privacy principles (ISO 29100), which, it says, were derived from existing principles developed by various states, countries and international organisations (ISO 2011). Although some might argue that the OECD Guidelines or the CoE's Convention are de facto international standards, the ISO's work is significant because it formulates information privacy principles as a standard that could have ubiquitous force, although its specific influence has yet to be seen. In any event, it has been 'adopted' for the purpose of this article. Its 11 privacy principles are briefly described below:

(1) *Consent and choice*: presenting to the PII 'data subject' the choice whether or not to allow the processing of her PII.
(2) *Purpose legitimacy and specification*: ensuring that the purpose(s) complies with applicable law.

(3) *Collection limitation*: limiting the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).
(4) *Data minimisation*: minimising the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who have access to it.
(5) *Use, retention and disclosure limitation*: limiting the use, retention and disclosure (including transfer) of PII to that which is necessary in order to fulfil specific, explicit and legitimate purposes.
(6) *Accuracy and quality*: ensuring that the PII processed is accurate, complete, up to date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use.
(7) *Openness, transparency and notice*: providing PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the processing of PII.
(8) *Individual participation and access*: giving data subjects the ability to access and review their PII, provided their identity is first authenticated.
(9) *Accountability*: assigning to a specified individual within the organisation the task of implementing the privacy-related policies, procedures and practices.
(10) *Information security*: protecting PII under an organisation's control with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and to protect it against risks such as unauthorised access, destruction, use, modification, disclosure or loss.
(11) *Privacy compliance*: verifying and demonstrating that the processing meets data protection and privacy safeguards (legislation and/or regulation) by periodically conducting audits using internal or trusted third-party auditors.

Other types of privacy

Several analytically discrete types of privacy are considered in this article. One type is information privacy, associated with data protection, but it is only one of several. We derive our typology from that articulated by Clarke (1997) and further elaborated by Finn, Wright, and Friedewald (2013).[9] Clarke identified four categories (or types) of privacy and outlined specific protections. His four categories are: privacy of the person; of behaviour; of data; and of communication. He notes 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'. Others, such as Solove (2006), have also developed a taxonomy of privacy; however, Solove's taxonomy focuses on potentially harmful or problematic activities affecting private matters or activities, rather than characterising types of privacy. Most of the items in his taxonomy are grounded in information privacy, although 'decisional interference' engages other types such as the body, the home, the family, and activities or practices related to these.

A variety of other multiple-category formulations can be found. A fourfold division of 'separate but related concepts' – information privacy, bodily privacy, privacy of communications, and territorial privacy – is used in a compendious international survey of

privacy laws and developments (Electronic Privacy Information Center and Privacy International 2007, 3). Different formulations appear in the PIA handbooks of Australia, Victoria State, Ontario and the United Kingdom. For example, the Office of the Victorian Privacy Commissioner states that '[t]he right to privacy in the Charter [of Human Rights and Responsibilities] covers not just information privacy, but bodily, territorial, locational and communications privacy' (OVPC 2009, 2). Similarly, the Ontario Information and Privacy Office PIA guide says that organisations should look at other types of privacy besides that of personal information: physical freedom from surveillance; person or personal space; communication; and the ability to control the sharing of their personal information (OCIPO 2010, 37).[10]

The UK Information Commissioner's Office's (ICO) PIA Handbook (version 2) provides more detail than the other privacy commissioners' guides with regard to each of the different types of privacy that closely resemble Clarke's schema (ICO 2009, 14). The Handbook describes each of these four types as follows:

Privacy of personal information is referred to variously as 'data privacy' and 'information privacy'. Individuals generally do not want data about themselves to be automatically available to other individuals and organisations. Even where data is possessed by another party, the individual should be able to exercise a substantial degree of control over that data and its use. The last six decades have seen the application of information technologies that in many ways have had substantial impacts on information privacy.

Privacy of the person, sometimes referred to as 'bodily privacy', is concerned with the integrity of the individual's body. At its broadest, it could be interpreted as extending to freedom from torture and right to medical treatment, but these are more commonly seen as separate human rights rather than as aspects of privacy. Issues that are more readily associated with privacy include body searches, compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement.

Privacy of personal behaviour relates to the observation of what individuals do, and includes such issues as optical surveillance and 'media privacy'. It could relate to matters such as sexual preferences and habits, political or trade union activities and religious practices. But the notion of 'private space' is vital to all aspects of behaviour, is relevant in 'private places' such as the home and the toilet cubicle, and is also relevant in 'public places', where casual observation by the few people in the vicinity is very different from systematic observation, the recording or transmission of images and sounds.

Privacy of personal communications could include various means of analysing or recording communications such as mail 'covers', the use of directional microphones and 'bugs' with or without recording apparatus and telephonic interception and recording. In recent years, concerns have arisen about third party access to email messages. Individuals generally desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations.[11]

It is important to identify and characterise the different types of privacy, as Finn, Wright, and Friedewald (2013) have done, because all types of privacy merit protection. In order to construct protections, the different types of privacy have to be identified and articulated. Clarke's four categories or types of privacy have generally been sufficient, but new technological, governmental and commercial developments have tested the limits of these four documents, unmanned aerial vehicles, second-generation DNA sequencing technologies, human-enhancement technologies and second-generation biometrics raise additional privacy

issues concerning not only the body and its movement, but the mind and space as well.[12] Such new technologies implicate several types of privacy that are partially reflected in the ICO's Handbook as well as in the philosophical, legal, and social science literature on privacy. Yet these types have become especially significant in recent years as a result of the development of technologies and – perhaps more importantly – of the new applications and purposes to which states and commercial organisations are finding for them. In some contexts, one may see overlaps with the conventional fourfold or other inventories of privacy types. As has been noted, existing regulatory practice does not altogether ignore these types as sources of issues that might be regulated under existing legal provision, although this goes against the grain of privacy-as-data-protection. But the additional types are sufficiently distinctive to provide a useful expansion of the scope of privacy protection. Distinguishing them helps to focus attention more systematically on novel threats and threats to broader dimensions of privacy that are created by the combination of technological capability and organizational policy and practice. Therefore, three other types of privacy should be added; namely, privacy of location and space; of thoughts and feelings; and of association (including group privacy).[13] Thus:

Privacy of location refers to the right of an individual to be present in a location or space without being tracked or monitored or without anyone knowing where he or she is. 'Space' could be physical or cyber space.

Privacy of thoughts and feelings is the counterpart to bodily privacy. Some scholars have identified what they call 'decisional privacy'. This is manifested in USA court decisions and legislation that, for example, give women the right to make decisions concerning their bodies, such as deciding whether to terminate a pregnancy. Such decisional privacy could be captured within or subsumed under the privacy of thoughts and feelings identified by Finn, Wright, and Friedewald (2013).

Privacy of association includes social and political relationships formed by people at different levels of scale, from the intimate to larger groups and collectivities.

We recognise that two or more types of privacy could be implicated by a new technology or service, such that some might see this as a blurring of types. Generally, however, we view privacy of personal behaviour as distinct from privacy of location. Privacy of behaviour means that one should be able to behave as one wishes without that behaviour being monitored. Privacy of location is different. It does not refer to behaviour or conduct within a space; it refers simply to the right of a person to travel through physical and cyber space without being tracked. To travel through cyber space means simply to surf the Internet without being tracked from one website to another.

There is a relationship among all seven types of privacy: they all relate to the individual's 'space', both internal and external, her functioning within that space and her relation- ship with others. Thus, there is a coherence and a comprehensiveness to the seven types or privacy that is often missing in other postulated types of privacy. While more than one type of privacy might be manifested, implicated or threatened in any form of behaviour or activity by the self or others, they are all compatible with Clarke's metaphorical definition of privacy as 'the interest that individuals have in sustaining a "personal space", free from interference by other people and organisations' (Clarke 2000, s. 2.1). Moreover, not only do the seven types speak to values pertaining to individuals, they also sustain social and political values that are

deeply rooted in pluralistic societies and liberal democracies. The seven types of privacy provide granularity and specificity to the notion of privacy rights. In other words, each of the seven types of privacy provides a basis for conceptualising a right to privacy – or, rather, several privacy rights.

Furthermore, the seven types of privacy provide a concrete basis for regulation and protection that is absent from more abstract conceptualisations of privacy. These seven types of privacy provide a useful basis for identifying, analysing and assessing privacy risks and harms and formulating protections for the various types of privacy by means of a more encompassing PIA than is generally used, in which data protection is at the forefront.[14] Most PIAs are actually DPIAs in the sense that they focus on data protection, rather than other types of privacy.

Additional privacy principles

It is important to formulate additional privacy principles that specifically address all types of privacy, in part because they provide a basis for considering the risks or harms that may arise to the individual, to groups and to society as a whole when one, or more, of these principles is violated. The additional privacy principles would be built upon the recognition that, in addition to the right to have their personal data or information privacy protected, people have further privacy rights that are worthy of protection against threats posed by surveillance even when no PII is processed; continuing the numbering from the ISO principles, these are:

(12) a right to dignity, i.e., freedom from infringements upon their person or reputation;[15]
(13) a right to be let alone (privacy of the home, etc.);[16]
(14) a right to anonymity, including the right to express one's views anonymously;[17]
(15) a right to autonomy, i.e., freedom of thought and action, without being surveilled;[18]
(16) a right to individuality and uniqueness of identity;[19]
(17) a right to assemble or associate with others, without being surveilled;
(18) a right to confidentiality and secrecy of communications;
(19) a right to travel (in physical or cyber space), without being surveilled;[20]
(20) a right not to have to pay in order to exercise their other rights of privacy (subject to any justifiable exceptions), and not to be denied goods or services on a less preferential basis.[21]

Some general remarks should be made at this point. First, some privacy rights can also function as privacy principles that can be used for identifying risks and harms. Privacy is a fundamental right in the EU by virtue of Article7 of the Charter of Fundamental Rights of the European Union, which states that '[e]veryone has the right to respect for his or her private and family life, home and communications.' A principle is a shared value, whereas a right is an entitlement; but they are mutually implicated. The ISO 29100 standard defines 'privacy principles' as a 'set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems'. While this definition is inadequate because it contextualises privacy principles as relating to PII only, insofar as the standard can recognise other types of privacy, the concise

definition of a privacy principle as a 'shared value' stands. Privacy standards can support privacy rights by providing a method to address privacy risks, but they cannot make mandatory a right to dignity or free speech. However, privacy standards can address privacy as a collection of rights and not simply the right of data protection. That some privacy rights can function as privacy principles makes them useful instruments on the basis of what questions can be formulated that will help understand whether a new technology or system might violate one of these principles. It is a structured way for assessing privacy risks in a more encompassing PIA, which is further discussed below.

Second, just as there are different types of privacy, so there is a collection of privacy rights, as identified above. The above rights offer more granularity as to what specifically is a privacy right. There may be other rights to privacy not identified as such here, but this list is relatively comprehensive at present. It is not intended to be systematic, but gives specificity to the right to privacy.

Third, which type or right of privacy should be regarded as on the same plane as another, or as a container for, or contained by, another, can be construed in different ways, and has been a matter of debate amongst theorists of privacy for a very long time (Schoeman 1986). A recent postulation is Marx's (2012, ix – xi) construction that locates anonymity within information privacy and as a condition for being let alone. He also sees information privacy as encompassing physical or bodily privacy as well as 'aesthetic privacy': sealing off certain private activities and unguarded moments from public view; this is akin to dignity. For him, information privacy is tied to spaces and places among a host of institutional and sectoral settings. But the history of privacy discourse shows that this is not the only possible 'take' on privacy, and that information privacy is not necessarily the only possible ruling paradigm.

Fourth, this list is more conveniently expressed in terms of rights that should be protected than in terms of what the state or the private sector should or should not do, in very specific terms, when handling personal data or engaging in other surveillance practices. The awkwardness of expression cannot be ignored, because principles must send a clear signal to the parties concerned about their activities, obligations, expectations, and remedies, and they must give a convincing account of why they should command compliance. A danger is that their enunciation may remain mere celebratory rhetoric without a cogent link to policy and practice. Nonetheless, it is likely that the 'legacy' principles of data protection, as embodied in the ISO principles, would lend themselves to rules and guidelines for surveillance practices (e.g., watching, tracking, data-mining, etc.) that infringe upon people's thoughts, spaces and associations. For example, the rules regarding consent, purposes, limitations, transparency and accountability seem directly applicable to forms of surveillance that threaten these rights, and could restrain the activities of surveillance practitioners whether or not PII is involved.

Fifth, although conflating rights and freedoms may be questionable, it is not unprecedented. The additional list springs from a recognition or assertion of rights that draws upon the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (usually termed the European Convention on Human Rights (ECHR)). This combines rights and freedoms, articulating several 'freedoms' including: thought, conscience and religion; expression;

assembly and association; and (in the 1963 Protocol No. 4) movement. There is also a 'right to liberty'. It is obvious that the list is not stated in the same form as the acquis of principles found in the OECD, CoE, APEC, ISO and other authoritative guidelines or 'principles' documents, not only because those principles relate to information privacy and therefore instruct data controllers about ethical and legal performance requirements – including their relationships with individuals – in processing personal data.

It is also because the additional rights or principles cannot so easily address specific persons or organisations whose activities might pose threats, because the threats are ubiquitous and their sources often not easily identifiable.

This, of course, in turn contributes to the difficulty of asserting these principles in the language of rights, as is done above, because the imposition of specific correlative obligations is indeterminate in some instances and does not obtain in others, depending upon the type of right in question (Wenar 2011). Nevertheless, here too, there is a precedent, as seen in the Australian Privacy Charter (APCC 1994). The Charter's principles are headed: consent; accountability; observance; openness; freedom from surveillance; privacy of communication; private space; physical privacy; anonymous transactions; col- lection limitation; information quality; access and correction; security; use and disclosure limitation; retention limitation; public registers; and 'no disadvantage' (no payment in order to exercise rights). The preamble to the APC elides the distinction between principles and rights by saying that their privacy principles 'comprise both the rights that each person is entitled to expect and protect, and the obligations of organisations and others to respect those rights'.22 The APC underpins its principles with rights, especially when it asserts that '[p]eople have a right to the privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about a person), and freedom from surveillance.' Moreover, it upholds autonomy, dignity, freedom of association, and free speech.

In any case, it goes without saying that – as with those that are already well established – any rights related to new principles or newly recognised types of privacy are not absolute, but can be overridden under strictly limited circumstances, as in Article 8(2) of the European Convention on Human Rights (CoE 1950); disputes over the applicability of these limitations in specific instances are subject to judicial decision.

Applicability of the privacy principles to the types of privacy

As a first step towards identifying risks to each type of privacy and ultimately indicating the measures that can be taken to avoid them, it is useful to construct a matrix showing the applicability of the various privacy principles – as construed here – to the seven types of privacy. Underlining the overlap among the principles and among the types of privacy, the matrix indicates that most principles are associated with more than one privacy type. In addition, the 'Xs' in the various cells should be regarded as indicative, rather than as definitive; in some instances, there may be different points of view about the applicability of some principles to some types of privacy. This is, in general, not significantly different from

the state of current discourse and jurisprudence, in which judgments vary about the practices that are covered by different, but related, legal or ethical precepts.

Table 1 aims to correlate privacy principles and types of privacy. Xs are in some cells and not in others because some principles are more closely correlated with particular types of privacy than others. For example, consent is a well-recognised principle in data protection, but it is not so well recognised in regard to other types of privacy. Similarly, transparency and notice do not generally apply, in our view, as principles of privacy of location because the right to privacy of location means that individuals have a right to be or travel somewhere (in physical and cyber space) without being monitored or tracked. However, it could be claimed that the principles of transparency and notice come into play even with privacy of location: for example, where one can be tracked in a city festooned with CCTV cameras.

Table 1. Privacy principles and types of privacy.

		Privacy of the person	Privacy of behaviour and action	Privacy of communication	Privacy of data and image	Privacy of location	Privacy of thoughts and feelings	Privacy of association
	Existing privacy principles							
1	Consent and choice	X			X			
2	Purpose legitimacy and specification	X		X	X	X		
3	Collection limitation	X		X	X	X		
4	Data minimisation			X	X	X		
5	Use, retention and disclosure limitation	X		X	X	X		
6	Accuracy and quality	X			X	X		
7	Openness, transparency and notice	X		X	X	X		
8	Individual participation and access				X	X		
9	Accountability	X		X	X	X		
10	Information security	X		X	X	X		
11	Privacy compliance	X		X	X	X		
	Other privacy principles							
12	Right to dignity, i.e., freedom from infringements upon their person or reputation	X	X	X	X	X	X	X
13	Right to be let alone (privacy of the home, etc.)	X	X	X	X	X	X	X
14	Right to anonymity, including the right to express one's views anonymously	X	X	X	X	X	X	X
15	Right to autonomy, to freedom of thought and action, without being surveilled		X	X			X	X
16	Right to individuality and uniqueness of identity	X					X	

(Continued)

Table 1. Continued.

		Privacy of the person	Privacy of behaviour and action	Privacy of communication	Privacy of data and image	Privacy of location	Privacy of thoughts and feelings	Privacy of association
17	Right to assemble or associate with others, without being surveilled		X					X
18	Right to confidentiality and secrecy of communications			X	X		X	X
19	Right to travel (in physical or cyber space), without being tracked		X			X		
20	People should not have to pay in order to exercise their rights of privacy (subject to any justifiable exceptions), nor be denied goods or services or offered them on a less preferential basis			X	X	X		X

Privacy risks and harms

In identifying additional principles associated with other types of privacy, it is useful to consider what is at stake when privacy is violated; therefore, typologies of privacy harms and risks could play an important part in further discussion. In practice, the notion of harm is familiar in information privacy law and discourse, whether in terms of privacy torts (intrusion; public disclosure of private facts; false light in the public eye; and appropriation) (Prosser 1960) or of the remedies available to data subjects whose privacy has been breached.[23]

RAND Europe's review of the EU Data Protection Directive leans heavily on advocating a harms-based approach in which risk is a prevailing concept for regulatory policy and practice (Robinson et al. 2009),[24] although this is a controversial move in a field in which the moral force of rights has taken precedence over the pragmatic (but nonetheless disputatious) determination of harms through assessing likelihood and severity. The scholarly literature includes Perri 6's look at privacy 'through the lens of risk', giving three general categories and specific enumerations: risks of injustice (significant inaccuracy; unjust inference; function creep; reversal of the presumption of innocence); risks to personal control over collection of personal information (excessive or unjustified surveillance; collection of data without the consent of the data subject; denial of access to the means of protecting oneself from any of these risks); and risks to dignity by exposure or embarrassment (absence of transparency; physical intrusion into space; absence of anonymity; unnecessary or unjustified disclosure or disclosure without consent) (6 1998). Solove expansively discerns 'four basic groups of harmful activities' involving information: collection (surveillance; interrogation); processing (aggregation; identification; insecurity; secondary use exclusion); dissemination (breach of confidentiality; disclosure; exposure; increased accessibility; blackmail; appropriation; distortion); and invasion (intrusion; decisional interference) (Solove 2006).25

It is important to note that this cornucopia of risk and harm classifications has been conceptualised largely within an information privacy framework with some extensions into other types. Nonetheless, the identification of additional principles could benefit from the discourse on harm and risk – even if the principles are stated in terms of rights rather than 'absence of harm' – as well as from traditional understandings of rights and liberties. One can plot the list of privacy principles against – once again – indicative and provisional examples of the harms and/or risks to individuals that could arise from their violation. The typology of risks used in this article has an affinity with 6's categories. From a table like that below, it is possible to develop risk-related questions that could be used in more sophisticated, more comprehensive PIA methodologies addressing all types of privacy rather than just information privacy, and showing impacts on entities beyond the individual person (Raab and Wright 2012; Wright and Raab 2012).

The function of Table 2 is to provide examples of risks or harms that could arise when a privacy principle is violated. It serves as a guide or explanation for policy-makers as well as technology developers and operators as it offers examples of harms to each of the listed privacy principles. Such tables can be and are used in PIA guidance documents. A company

or government agency aiming at legal and ethical compliance might wish to use, or to construct, such a table. As part of the PIA process, such a table could help ensure that a newly envisaged technology or system is not developed in a way that intrudes upon the different types of privacy and principles.

This table is not intended to be a comprehensive risk-mapping tool; it is indicative, not definitive, and can support PIA and SIA methods. The value it adds to existing methods is its more systematic, structured approach to privacy risk identification, assessment and management. The more encompassing PIA that we propose is an innovation.

Table 2. Privacy principles and examples of risks or harms.

	Existing privacy principles	Examples of main risks or harms
1	Consent and choice	The person is not given a meaningful choice; her consent is not obtained (lack of consent: risk to personal control)
2	Purpose legitimacy and specification	The purposes of the technology may not comply with applicable law; use of a technology may exceed what is legitimate or specified (excessive or unjustified surveillance: risk to personal control)
3	Collection limitation	More data is collected than necessary which enables governments or companies to intrude upon the individual's privacy (excessive or unjustified surveillance: risk to personal control)
4	Data minimisation	A company may share data gathered from or about an individual with its corporate allies (function creep or unjust inferences: risk of injustice)
5	Use, retention and disclosure limitation	PII is held longer than necessary, e.g., communications records or DNA of those not charged with an offence (excessive surveillance and inaccuracy, lack of anonymity: risk of injustice, risk to personal control and risk to dignity)
6	Accuracy and quality	A company or government may hold incorrect data about an individual which puts her on a 'no-fly' list, for example (inaccuracy and reversal of presumption of innocence: risk of injustice and risk to dignity)
7	Openness, transparency and notice	A company may collect a person's PII but may not tell her (or anyone) how her data is being used (lack of transparency: risk of injustice and risk to dignity)
8	Individual participation and access	A company may collect PII but not allow the individual to access her records (inaccuracy and lack of transparency: risk of injustice, risk to personal control and risk to dignity)
9	Accountability	The organisation has not assigned accountability to anyone, hence, everyone shirks their responsibility for adhering to privacy and/or data protection legislation (a variety of harms: risk of injustice, risk to personal control and risk to dignity)
10	Information security	The organisation does not take proper care for ensuring the security of data, which leads to employees' losing PII as well as data breaches (failure of confidentiality: risk to personal control and risk to dignity)
11	Privacy compliance	The organisation does not adequately comply with data protection legislation and has not subjected itself to independent third-party review or audit (a variety of harms: risk of injustice, risk to personal control and risk to dignity)

(Continued)

Table 2. Continued.

	Other privacy principles	Examples of main risks or harms
12	Right to dignity, i.e., freedom from infringements upon the person or her reputation	Airport authorities may require travellers to submit to a body scan if they wish to fly (physical intrusion, reversal of presumption of innocence, lack of genuine consent: risk of injustice, risk to personal control and risk to dignity)
13	Right to be let alone (privacy of the home, etc.)	Governments, companies and malicious persons may be constantly trying to find out what a person is doing or thinking or where she is going. Marketers may call, contact or otherwise spam people to sell them something (lack of anonymity, lack of consent, intrusiveness: risk to personal control and risk to dignity)
14	Right to anonymity, including the right to express one's views anonymously	With facial recognition, anonymous speech in public places may be impossible; governments, companies, law enforcement authorities, intelligence agencies and miscreants may try to determine who expressed what views on the Internet (lack of anonymity: risk to dignity)
15	ight to autonomy, to freedom of thought and action, without being surveilled	New technologies may infer a person's emotional state or even what thoughts cross her mind; other technologies may influence her behaviour, attitudes, views (inaccuracy, lack of consent, intrusiveness: risk to personal control and risk to dignity)
16	Right to individuality and uniqueness of identity	Social sorting and profiling may stereotype people; a person may try to express her individuality, but governments and companies may try to influence her or limit her choices and thus her life chances (unjust inference, excessive or unjustified surveillance: risk of injustice, risk to personal control and risk to dignity)
17	Right to assemble or associate with others without being surveilled	The pervasiveness of CCTV makes it difficult or impossible for a person to associate with others without the knowledge of state agencies or companies (lack of anonymity, unjust inference: risk of injustice and risk to dignity)
18	Right to confidentiality and secrecy of communications	Intelligence agencies may monitor many people's communications without a warrant (lack of confidentiality, excessive surveillance: risk to personal control and risk to dignity)
19	Right to travel (in physical or cyber space) without being tracked	Facebook used its Beacon 'service' to alert associates about users' likes and preferences without their consent or knowledge; Google created the Buzz social network based on people's emails without telling them or seeking their consent in advance (lack of consent and transparency: risk to personal control and risk to dignity)
20	People should not have to pay in order to exercise their rights of privacy (subject to any justifiable exceptions), nor be denied goods or services or offered them on a less preferential basis	Targeted advertising may mean that some consumers pay more for the same service than others

Decision-makers would do well to avoid a strictly compliance-based approach to privacy risk. At a time when privacy appears to be threatened more than ever before, and by novel kinds of surveillance, further guidance could be given to industry and others to uncover privacy risks by using sets of questions to identify privacy risks, rather than ticking some boxes on a form. While organisational project managers and decision- makers may find it useful to consider and comply with the privacy principles listed in this article in the development of new projects, services, applications, products, proposed legislation or other initiatives, project managers or decision-makers should not lose sight of the primary objective, which is to identify and resolve privacy risks before they materialise.

PIA methodology prompts an important but infrequently asked question (Raab 2005): should a surveillance technology or system be considered privacy-safe until proven dangerous, or dangerous until proven safe? PIA may require a reasonable demonstration of the latter; laws and litigation may be based on the former. PIA concentrates minds upon the question of the privacy risks people face. If such questioning can take the practice and theory of privacy protection beyond a merely casual use of the term 'risk', it could perform an overdue service. Whatever the ambiguity of applying risk analysis to the privacy implications of technological design and application, risk assessment may thus help data controllers, regulators, PIA practitioners and the public to a better understanding and to a more fully informed privacy debate.

Conclusion: Why we need to debate privacy principles

It is useful to generate debate about these principles and harms for at least four main reasons. First, it will help to refocus the attention of policy-makers, regulators, academics and advocates away from only, or primarily, data protection to the detriment of other types of privacy and privacy rights, which may be affected by policies and practices. Privacy and data protection are each accorded an article (7 and 8 respectively) in the Charter of Fundamental Rights of the European Union (European Parliament, the Council and the Commission 2000), so there should in theory be parity between these two rights. However, such is not the case in the EU, which has a Data Protection Directive (95/46/EC) and a proposal for a Data Protection Regulation, but it does not have a Privacy Directive or Privacy Regulation. The EU has an Article 29 Data Protection Working Party (which is expected to evolve into a European Data Protection Board), and Member States have Data Protection Authorities (DPAs) – regulatory agencies that elsewhere in the world are termed Privacy Commissioners.[26]

These are only in part semantic examples; they highlight the reality of what 'privacy' protection has come to mean. González Fuster and her colleagues write,

> *Practices that do not constitute a personal data protection issue strictu sensu can still represent an infringement of the right to privacy* – and vice versa. EU institutions should never limit the assessment of the impact on fundamental rights of security measures that comprise the processing of personal data to an assessment of their compliance with data protection law. (González Fuster, De Hert and Gutwirth 2011: 4; emphasis added)

Clarke has also decried the ‘serious debasement of the term “privacy” ...[where it has been equated]... with the highly restrictive idea of “data protection”’ (Clarke 2006). Cate has made a somewhat similar observation: ‘Modern privacy law… has substituted individual control of information, which it in fact rarely achieves, for privacy protection’ (Cate 2006, 374). Although some DPAs have dismissed the difference between data protection and privacy as so much semantic posturing, they have sometimes addressed technologies that pose risks to types of privacy other than data protection: body scanners are an example (Article 29 Working Party 2009) of a technology that impacts privacy of the person, which is not a violation of information privacy unless the scanners process personal information. The same is true of surveillance drones that impact privacy of behaviour. Expanding the array of privacy principles helps to achieve a better relationship between a procedural approach to information privacy and a human rights approach.

Second, formulating privacy principles (rights, freedoms) and indicating the harms that arise when they are violated is of critical importance at a time when PIA and/or DPIA may become mandatory, as set out in Article 33 in the European Commission’s pro- posed Data Protection Regulation. PIA is an important instrument to identify privacy risks and ways of avoiding, minimising, retaining or sharing them. The term ‘PIA’ has been used around the world, although its application to only data protection has some unfortunate consequences. For example, when identifying privacy ‘targets’ (an unfortunate term), the industry-dominated group developing an RFID PIA framework chose only the data protection principles in the EU Data Protection Directive (Spiekermann 2012). If RFID applications raise other privacy issues beyond compliance with data protection principles, they are likely to be overlooked. Just when arguments for overcoming this restriction have come into view (Wright and Raab 2012), the European Commission has introduced the term DPIA in the proposed Regulation, which might underline the limited focus and suggest to some that the Commission is less interested in broad-based rights assessments of the impacts on privacy of new technologies or other initiatives than it is on their impact on data protection. Hence, it is important that PIA, to be fully effective, addresses all types of privacy and the associated privacy principles, and the risk of harm to a wider array of rights. Any future revision of ISO 29100 could also take into account the suggestions made in this article.

Third, European policy-makers and other stakeholders might consider the status of Article 7 (private and family life) of the Charter now that Article 8 grants the new right to data protection. This has traditionally been implemented under ‘privacy’ rights in other totemic documents in this field, such as Article 8 of the ECHR, and therefore the primary focus on data protection in Europe has drawn attention away from other types of privacy impacted by technological change, government policy and commercial practice. A step toward the recalibration of the relationship between data protection and privacy could be to recognise the different types of privacy – as the ICO did in its version 2 PIA Handbook, for example – and, in doing so, to consider the privacy principles with which they are associated. Privacy regulation could and should be based on Article 7 of the Charter of Fundamental Rights of the European Union as well as Article 16 of the Lisbon Treaty.

We recognise that there could be a risk that, if one brings too many aspects under the umbrella of privacy, the term could become meaningless and lose its power to safeguard a core of privacy protection. However, the motivation of this article is the recognition of the need to reinforce the protection of other types of privacy that are less well protected now. Some types of privacy – for example, privacy of location – are severely threatened by technological, business, and government policy developments, especially with regard to national security and law enforcement. Adequate protection of all types of privacy is essential if we are to resist the ubiquity of surveillance systems that undermine democracy and the rule of law.

Coda

Finally, we add a brief status report, with reference to developments that are underway at the time of writing. PIAs are explicitly mandatory in the UK, but only for the public sector, although the public sector in some cases is now requiring private sector suppliers to do PIAs too. The UK ICO PIA Handbook explicitly, and in some detail, mentions four types of privacy. If the proposed Data Protection Regulation is adopted, DPIAs will become mandatory where specific risks are present. In reality, we think many organisations will do PIAs anyway. The process of conducting a PIA and a DPIA is more or less the same; the principal difference is in scope. A PIA has a wider scope, up to seven types of privacy to consider. The need for a more encompassing PIA method is apparent when one considers some of the examples mentioned above, for example, body scanners impact privacy of the person and drones impact privacy of behaviour. Since the Snowden revelations, most companies are much more aware of the need to conduct proper PIAs, because large swaths of the public do not trust them. In the ISO's process of finalising a draft PIA standard, the ideal would be to have a legislative provision for PIA, but that is unlikely to happen at the European level at this time.

A suitable legal basis for a mandatory PIA would be an amendment to the proposed Data Protection Regulation. A separate Regulation devoted to other types of privacy would be even better. However, a new piece of legislation devoted to privacy would take some years to develop, adopt and bring into force. The ISO is well along in the development of a PIA standard, which we expect to be adopted in 2015. Although it too has a focus on data protection, it does explicitly mention other types of privacy.

Acknowledgement

We gratefully acknowledge comments made on an earlier draft of this article by members of the IFIP Summer School on Privacy and Identity Management 2013, Nijmegen, The Netherlands, 21 June 2013, as well as by the two anonymous reviewers. We thank in particular the reviewer who was concerned about a suitable legal basis for PIA.

Notes

1. In addition to the documents described here, other examples include Scottish Government (2011), Marx (1998) and Pounder (2008).
2. The HEW report was one of the first such reports, but by no means the first, as its Appendix B makes clear. Even earlier initiatives had been undertaken in the UK, Canada and some other countries. See, for example, Home Office (1972) and Task Force on Privacy and Computers (1972).
3. Space limitations prevent full description of these principles.
4. OECD (1980, General Background, para 38).
5. This article does not deal with recent revisions of the OECD and CoE documents.
6. Further discussion of old and new principles can be found in Raab (2012).
7. The New Act also significantly strengthens the powers of the Australian Information Commissioner to conduct investigations and ensure compliance with the amended Privacy Act. See DLA Piper, Data Protection Laws of the World, March 2013, pp. 11 – 12. See also Talevski and Osman (2013).
8. See Part 2, section 6 of the Act. http://www.legislation.govt.nz/act/public/1993/0028/latest/viewpdf.aspx
9. 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 is used in the PIA adopted by various privacy regulators in Australia, Canada, New Zealand, the UK and Ireland.
10. The last-named item is often called 'informational self-determination', a pillar of information privacy protection in Germany.
11. However, the ICO's new PIA code of practice, adopted in March 2014 (ICO 2014) following a four-month consultation period, has reduced the types of privacy to two, i.e., information privacy and physical privacy. The consultation was carried out between August and November 2013. Information Commissioner's Office (ICO), 'Privacy impact assessments code published', News release, 25 Feb 2014. http://ico.org.uk/news/latest_news/2014/privacy-impact-assessments-code-published.
12. Gary T. Marx (1998) reflects these changes in his articulation of a 'new ethics of surveillance', but his focus is predominantly upon surveillance as involving personal data collection, the province of traditional privacy law and regulation.
13. For a more detailed exegesis of the seven types, see Finn et al. (2013).
14. For a review of publicly available PIA reports in the UK, see Wright (2014).
15. The right to dignity is proclaimed in Article 1 of the Charter of Fundamental Rights of the European Union: 'Human dignity is inviolable. It must be respected and protected.'http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:0391:0407:EN:PDF
16. See Principle 8 in the Australian Privacy Charter: 'Private space – People have a right to private space in which to conduct their personal affairs. This right applies not only in a person's home, but also, to varying degrees, in the workplace, the use of recreational facilities and public places.' Jacoby says similarly: 'The concept of

"home" or living quarters has been construed broadly to be understood as any domain of privacy' (Jacoby 2007: 457). The 'right to be let alone' is the oldest and best-known definition of privacy. However, its applicability today is wider than was the case back in 1890 when Warren and Brandeis penned their classic essay. We interpret the right to be let alone as covering, for example, not being subjected to unsolicited marketing telephone calls, not being videoed every time one talks to a friend in a bar, not being tracked wherever one drives one's car or every time one turns on one's computer, not being required to go through a body scanner, etc. In other words, the right to be let alone is applicable to all seven types of privacy.

17. See Principle 10 in the Australian Privacy Charter: 'Anonymous transactions – People should have the option of not identifying themselves when entering transactions.' This is only one example of anonymity.
18. 'Individuals not only need to be able to be alone with their own thoughts, but they also need to be free to share those thoughts with others without being subject to the watchful, possibly critical, eye of the state… By ensuring that there is a limit on what the state can know about us, privacy not only helps to protect individual autonomy, but also leaves us free to use that autonomy in the exercise of other fundamental rights like the right to free speech' (Goold 2010, 43). See also Principle 6 of the Australian Privacy Charter: 'Freedom from surveillance – People have a right to conduct their affairs free from surveillance or fear of surveillance. "Surveillance" means the systematic observation or recording of one or more people's behaviour, communications, or personal information.' http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1876069
19. This is an anti-discrimination principle, because profiling and social sorting pose threats to individuality.
20. Principle 8 in the Australian Privacy Charter relates to this, although not to travel or movement as such: 'Private space – People have a right to private space in which to conduct their personal affairs. This right applies not only in a person's home, but also, to varying degrees, in the workplace, the use of recreational facilities and public places.'
21. This principle has been adapted from Principle 18 in the Australian Privacy Charter: 'No disadvantage'.
22. http://www.privacy.org.au/About/PrivacyCharter.html. The Charter was produced by the Australian Privacy Charter Council (APCC), a civil society group.
23. See, for example, 'damage' and 'distress' in the UK Data Protection Act 1998, § 13.
24. This was prepared for the UK Information Commissioner's Office.
25. As Calo has shown, with reference to Solove, there are still further complications – and scholarly disagreements – in discussing privacy harms and risks. These relate to how the boundaries are drawn round what is, or is not, a privacy harm (the need for a 'rule of recognition' to determine the limits; and the relationship between subjective (perceptions of loss of control, resulting in fear or discomfort) and objective (actual adverse consequences) categories of harm (Calo 2011). The present article does not address these and other issues in the understanding of risk and harm.

26. A further point in the same vein can be made: in data protection legislation, the individual is referred to as a 'data subject' – a depersonalised term that strips the individual of her individuality, as though she were only a set of 1s and 0s. At the EC level, there appear to be few policy documents focused on other types of privacy as distinct from data protection.

References

6, P. 1998. *The Future of Privacy, Volume 1: Private Life and Public Policy*. London: Demos, pp. 39 – 42.

Article 29 Data Protection Working Party. (2009). Letter to the European Commission, Brussels, 11 February. Accessed June 22, 2013. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2009_05_11_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf

Asia-Pacific Economic Cooperation. 2005. APEC Privacy Framework, APEC Secretariat, Singapore. Accessed June 22, 2013. http://publications.apec.org/publication-detail.php?pub_id=390

APCC (Australian Privacy Charter Council). 1994. Australian Privacy Charter, December. [Online] Accessed June 22, 2013. http://www.privacy.org.au/About/PrivacyCharter.html

Bennett, C. J. 2011. "In Defence of Privacy: The Concept and the Regime." *Surveillance and Society* 8 (4): 485 – 496.

Bennett, C. J., and C. D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: The MIT Press.

Bennett, C. J., and R. Grant. 1999. "Introduction." In *Visions of Privacy: Policy Choices for the Digital Age*, edited by C. J. Bennett and R. Grant. Toronto: University of Toronto Press: 3 – 16.

Calo, M. R. 2011. "The Boundaries of Privacy Harm." *Indiana Law Journal* 86 (3): 1130 – 1162.

Canadian Standards Association. 1996. Model Code for the Protection of Personal Information, CAN/ CSA-Q830 – 95, March. [Online] Accessed June 22, 2013. http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code

Cate, F. H. 2006. "The Failure of Fair Information Principles." In *Consumer Protection in the Age of the Information Economy*, edited by J. K. Winn. Ashgate: 341 – 378.

Clarke, R. 1997. "Introduction to Dataveillance and Information Privacy, and Definitions of Terms." Xamax Consultancy, Aug. [Online] Accessed June 22, 2013. http://www.rogerclarke.com/DV/Intro.html

Clarke, R. 2000. “Beyond the OECD Guidelines: Privacy Protection for the 21st Century.” Xamax Consultancy, 4 Jan. Accessed June 22, 2013. http://www.rogerclarke.com/DV/PP21C.html

Clarke, R. 2006. “What’s “Privacy”?.” Version of 7 August. Accessed June 22, 2013. http://www. rogerclarke.com/DV/Privacy.html

CoE (Council of Europe). 1950. Convention for the Protection of Human Rights and Fundamental

Freedoms (European Convention on Human Rights (ECHR)), Strasbourg. Accessed June 22, 2013. http://www.echr.coe.int/Documents/Convention_ENG.pdf

CoE (Council of Europe). 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January. Accessed June 22, 2013. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

DLA Piper, *Data Protection Laws of the World*, March 2013.

Electronic Privacy Information Center and Privacy International. 2007. *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments*. Washington DC and London: Electronic Privacy Information Center and Privacy International.

European Parliament and the Council. 1995. 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, 23 November, pp. 0031 – 0050 (22 June 2013).

European Parliament, the Council and the Commission, Charter of Fundamental Rights of the European Union, 2000/C 364/01. Official Journal of the European Communities, C 364/1 – 22, 18.12. 2000. Accessed April 26, 2014. http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Finn, R., D. Wright, and M. Friedewald. 2013. “Seven Types of Privacy.” In European Data Protection: Coming of Age?, edited by S. Gutwirth, R. Leenes, P. De Hert et al. Dordrecht: Springer: 3 – 32.

González Fuster, G., P. De Hert, and S. Gutwirth. 2011. “Privacy and Data Protection in the EU- Security Continuum.” IN:EX/CEPS Policy Briefs, No. 12, 2011. Accessed June 22, 2013. http://works.bepress.com/serge_gutwirth/71

Goold, B. 2010. “How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy.” In *Surveillance in a Constitutional Government*, edited by D. W. Schartum, 38 – 48. Fagbokforlaget.

HEW (US Department of Health Education and Welfare). 1973. *Records, Computers and the Rights of Citizens*. Washington, DC: Report of the Secretary’s Advisory Committee on

Automated Personal Data Systems. July. [Online] Accessed June 22, 2013. http://epic.org/privacy/hew1973report/

Home Office. 1972. Report of the Committee on Privacy. London: Rt. Hon. Kenneth Younger, Chairman, HMSO.

ICO (Information Commissioner's Office). 2009. Privacy Impact Assessment Handbook, Version 2.0, Cheshire, UK: Wilmslow. June.

ICO (Information Commissioner's Office). 2014. "Privacy impact assessments code published", News release, Feb 25. http://ico.org.uk/news/latest_news/2014/privacy-impact-assessments- code-published

ISO (International Organization for Standardization). 2011. *Information technology — Security techniques — Privacy framework, ISO/IEC 29100*. 1st ed. Geneva: International Standard. 15 Dec.

Jacoby, N. 2007. "Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States." *Georgia Journal of International and Comparative Law* 35 (3): 433 – 493.

Marx, G. T. 1998. "An Ethics for the New Surveillance." *The Information Society* 14 (3): 171 – 186.

Marx, G. T. 2012. "Privacy is Not Quite Like the Weather." In *Privacy Impact Assessment*, edited by D. Wright and P. De Hert, v – xiv. Dordrecht: Springer.

OCIPO (Office of the Chief Information and Privacy Officer). 2010. Privacy Impact Assessment Guide for the Ontario Public Service. Queen's Printer for Ontario.

OECD (Organisation for Economic Co-operation and Development). 1980. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris, 23 September. Accessed June 22, 2013. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacy andtransborderflowsofpersonaldata.htm#recommendation

OVPC (Office of the Victorian Privacy Commissioner). 2009. Privacy Impact Assessments, A guide for the Victorian Public Sector, Edition 2, April.

Prosser, W. L. 1960. "Privacy." *California Law Review* 48 (3): 383 – 423.

Pounder, C. 2008. "Nine Principles for Assessing Whether Privacy is Protected in a Surveillance Society." IDIS 1 (1): 1 – 22.

Raab, C. 2005. "The Future of Privacy Protection." In *Trust and Crime in Information Societies*, edited by R. Mansell and B. Collins, 282 – 318. Cheltenham: Edward Elgar.

Raab, C. 2012. “Regulating Surveillance: The Importance of Principles.” In *Routledge Handbook of Surveillance Studies*, edited by K. Ball, K. D. Haggerty, and D. Lyon, 377 – 385. London: Routledge.

Raab, C., and D. Wright. 2012. “Surveillance: Extending the Limits of Privacy Impact Assessment.” In *Privacy Impact Assessment*, edited by D. Wright and P. De Hert, 363 – 383. Dordrecht: Springer. Robinson, N., H. Graux, M. Botterman, and L. Valeri. 2009. Review of the EU Data Protection Directive. Cambridge: RAND Europe.

Schoeman, F. D., ed. 1986. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.

Scottish Government. 2011. Identity Management and Privacy Principles. http://www.scotland.gov.uk/Publications/2010/12/PrivacyPrinciples

Solove, D. J. 2006. “A Taxonomy of Privacy.” *University of Pennsylvania Law Review* 154 (3): 477 –560.

Spiekermann, S. 2012. “The RFID PIA – Developed by Industry, Endorsed by Regulators.” In *Privacy Impact Assessment*, edited by D. Wright and P. De Hert, 323 – 346. Dordrecht: Springer.

Talevski, J., and H. Osman. 2013. “Privacy Act Reforms to Hit.” PC Advisor, 6 June. Accessed June 22, 2013. http://www.pcadvisor.co.uk/news/network-wifi/3451166/privacy-act-reforms-to-hit/

Task Force on Privacy and Computers. 1972. *Privacy and Computers*. Ottawa: Departments of Communication and Justice, Information Canada.

Wenar, L. 2011. “Rights.” In *The Stanford Encyclopedia of Philosophy* (Fall 2011 Edition), edited by E. N. Zalta. Accessed June 22, 2013. http://plato.stanford.edu/archives/fall2011/entries/rights/

Wright, D. 2014. "How Good are PIA Reports and Where are They?." *European Business Law Review* 26 (3), May.

Wright, D., and C. Raab. 2012. "Constructing a Surveillance Impact Assessment." *Computer Law & Security Review* 28 (6): 613 – 626.