FEATURE

Protecting The Privacy of Library Users

Author _ Paul Pedley (paul.pedley@gmail.com), Head of Research at the Economist Intelligence Unit. Previously Paul was Library and Information Services Manager at the law firm Theodore Goddard. Paul has also worked for the developers of Canary Wharf in London's docklands and in government libraries at the Department of Trade and Industry, the Office of Telecommunications (OFTEL) and the Property Services Agency.

The purpose of this paper is to consider the best way of understanding the concept of informational privacy, including a discussion of what would be an appropriate theoretical framework and useful conceptual model; as well as how such a model can be used to investigate specific issues of library privacy.

Two methodologies were used for the research: a literature review, and a thematic analysis of three pieces of data protection legislation. The research project is still in its relatively early stages, and the intention is to use several other methodologies to test the initial findings.

Informational privacy is a derivative layer of other forms of privacy, and as such can only be properly understood in relation to each of the underlying privacy types. Where libraries rely for the delivery of their services on digital technologies provided by external vendors, they need to better understand whether and how those technologies impact upon each of the different types of privacy identified by (Koops et al. 2017).

Using three pieces of data protection legislation to identify key themes does not give a complete picture of informational privacy; nor does it fully address the wider privacy implications. A detailed review of relevant case law on privacy from the European Court of Human Rights was not undertaken as part of this project. The choice of words and phrases appearing in data protection legislation and the subsequent grouping of them into broad themes is subjective.

The observation that all library privacy scenarios have an informational privacy component alongside one or more privacy types has significant implications for information professionals intending to protect the privacy of their users; because, if correct, it means that simply complying with data protection laws does not fully address the protection of the underlying privacy types.

Protecting user privacy and confidentiality has long been an integral part of the mission of libraries. Caldwell-Stone (2012) defines library users' information privacy as the right to read and inquire anything, without the fear of being judged or punished. It is relevant to both bricks and mortar and digital libraries.

Library privacy is important because of the "chilling effect" whereby users either know or suspect that they are being monitored and change their behavior accordingly. The "chilling effect" threatens the ability of library users to explore difficult, controversial, or potentially embarrassing topics without fear of being judged.

Gorman (2000) identifies privacy as one of eight enduring values of librarians and believes that this consists of ensuring the confidentiality of records of library use and overcoming technological invasions of library use.

"Although privacy is one of the core tenets of librarianship, technology changes have made it increasingly difficult for libraries to ensure the privacy of their patrons in the twenty-first century library" (Newman and Tijerna 2017, ix).

Is it possible for librarians to protect the privacy of their users, and if so, how? If, for example, a library user accesses an ebook from home, their personal data is processed by the library; by the e-book vendor; by the e-reader software company; and possibly even by illegal entities.

Libraries rely on commercial products from external vendors to provide their services. Indeed Barron and Preater (2018, 87) say "Contemporary librarianship, as practitioners have constructed it, could not exist without library systems." Technologies used include integrated library systems, discovery services, commercial products offering electronic newspapers, magazines, and e-books. Libraries have contracts in place with vendors, but not necessarily with everyone in the supply chain. For example, users may access e-book content through a third-party's software (such as Adobe Digital Editions) with whom the library has no formal contract.

Examples of the privacy of library users being threatened include:

- The British Library withstood a brute force attack on its systems over a four-day period in which the attacker attempted to obtain customer data.The attack was unsuccessful and no data was lost (British Library 2016).
- Students were warned that some of their data may have been compromised after a breach at Trinity College Dublin's library (McLysaght 2011).
- Keystroke logging devices were found on several computers in Cheshire libraries (BBC News Online 2011).
- Borrower records of 20 Fingal library users had been edited to contain data of a highly inappropriate, sexually explicit nature (Halpin 2018).

"Libraries and librarians have embraced technological changes in order to offer faster, more accurate, and easier-to-access materials and information to patrons. But with these technological advances came an increased ability to intrude on the intellectual privacy of library patrons by both libraries and the vendors they contract with for patron services" (Newman and Tijerna 2017, 1).

How Best Can We Understand Informational Privacy?

Westin (1967) defined informational privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others." Westin's definition is well suited to the 1960's era from which it comes, because individuals typically provided their own data to organisations. However, half a century later, a significant proportion of data about identifiable individuals is gathered by other means: it is often observed, derived or inferred (Abrams 2016, 6–8).

Many scholars focus on informational privacy in terms of ownership and control. For example, Branscomb generated a list of information rights which includes the right to control the release of information and the right to withhold information about ourselves (Branscomb 1985, 81). Gorman (2000, 144) says that "our informational privacy is the right to control personal information and to hold our retrieval and use of recorded knowledge to ourselves, without such use being monitored by others." Floridi (2016), however, believes privacy should be anchored around human dignity rather than ownership and control. We would go further and say that one should ask whether the result of someone processing personal data results in a violation of the human dignity of one or more individuals, thereby focussing on outcomes rather than intentions. In a world characterised by big data and algorithms it is only possible to identify patterns such as discrimination on the grounds of race, sexual orientation, gender, or religious beliefs if one views things from the wider group perspective.

Data protection laws are focussed on protecting the personal information of identified or identifiable individuals, and as such represent the procedural means through which the substantive right to informational privacy is enforced. But that raises the question as to whether data protection laws provide a satisfactory procedural means for comprehensively protecting an individual's privacy. To learn how we can best understand informational privacy, we must consider informational privacy within its wider context.

Data protection is not a direct equivalent for privacy (Wright and Raab 2014, 16). Several scholars have looked at the distinction between privacy and data protection. (Kokott and Sobotta 2013) consider the overlaps as well as the significant differences between the right to data protection and the right to privacy by looking at the two underlying systems of fundamental rights protection (the EU Charter of Fundamental Rights and the European Convention on Human Rights). The Charter clearly distinguishes between data protection and privacy: Article 7 covers respect for private and family life whereas article 8 covers protection of personal data. The European Convention on Human Rights and the General Data Protection Regulation (GDPR) do not contain similar distinctions.

Gellert and Gutwirth (2013, 529) examine the rights to privacy and data protection, and they apply the scope of these rights to three case studies: body-scanners, human enhancement technologies such as brain computer interface and neuro-enhancement, and genome sequencing. They found that even when both rights apply to the same situation, they do not always result in precisely the same legal outcome in terms of the legality of the situation.

The goal of data protection is not the protection of data but of the individuals to whom the data refer (Gutwirth et al. 2014, 222). Meanwhile the right to privacy as enshrined in the European Convention on Human Rights is a four-folded right covering private life, family life, home, and correspondence (Gutwirth et al. 2011).

Gellert and Gutwirth (2013) make a number of distinctions between data protection and privacy:

- Data protection and privacy differ both formally and substantially, although there are overlaps.
- Data protection is broader because it applies automatically each time personal data are processed whereas privacy is only triggered if there has been an interference with one's right to privacy.
- Data protection is narrower because it only deals with the processing of personal data, whereas privacy applies to the processing of personal and non-personal data where it affects one's privacy.
- The proportionality tests for the right to privacy and the right to the protection of personal data may well diverge.

Privacy types

Following in the footsteps of Blok (2002), Koops et al. (2017) believe informational privacy can be seen as a derivative or added layer of, or perhaps precondition to, other forms of privacy. This leads them to treat informational privacy not as a privacy type but as an overlay related to each of the underlying privacy types.

Many scholars have built on one another's work to develop and refine lists of privacy types. According to Finn et al. (2013, 1), Clarke was "the first privacy scholar of whom we are aware to have categorised the types of privacy in a logical, structured, coherent way," citing Clarke (1997). However, we would point to two earlier categorizations.

Westin (1967, 35–42) identified four functions of privacy: personal autonomy, emotional release, self-evaluation, and limited and protected communication. Westin also expressed his ideas in terms of four states of privacy: solitude, intimacy, anonymity, and reserve.

Pedersen (1979) identified six types of privacy:

1. Reserve,
2. Isolation,
3. Solitude,
4. Intimacy with Family,
5. Intimacy with Friends, and
6. Anonymity.

He also undertook a factor analysis of ratings within each privacy type to find types of privacy functions (147). The factors found were

1. Contemplation,
2. Autonomy,
3. Rejuvenation,
4. Confiding,
5. Creativity,
6. Disapproved consumptions,
7. Recovery,
8. Catharsis, and
9. Concealment.

Clarke (1997) defined four types of privacy, adding a fifth in 2013:

1. privacy of the person (bodily privacy),
2. privacy of personal data (which is one component of informational privacy),
3. privacy of personal behaviour (restrict information about personal matters such as religious practices, sexual practices, or political activities),
4. privacy of personal communication (restriction on monitoring telephone, e-mail and virtual communications, another component of informational privacy), and

	Personal zone "solitude"	Intimate zone "intimacy"	Semi-private zone "secrecy"	Public zone "inconspicuousness"
(Emphasis on) freedom from "being let alone"	Bodily privacy	Spatial privacy	Communicational privacy	Proprietary privacy
(Emphasis on) freedom to "self-development"	Intellectual privacy	Decisional privacy	Associational privacy	Behavioral privacy

Figure 1. Typology of privacy by Koops et al 2017

5. privacy of personal experience (added in 2013, since many of our experiences in contemporary society are mediated through screens, which produce media that shape our experiences).

Finn et al. (2013) expanded Clarke's list of privacy types based on the impact of six new and emerging technologies:

1. whole body imaging scanners,
2. RFID-enabled travel documents,
3. unmanned aerial vehicles,
4. second-generation DNA sequencing technologies,
5. human enhancement technologies, and
6. second-generation biometrics.

Their expanded list consists of seven types of privacy:

1. privacy of the person,
2. privacy of behaviour and action,
3. privacy of personal communication,
4. *privacy of data and image* (ensuring 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)
5. *privacy of thoughts and feelings* (thought does not automatically translate into behavior),
6. *privacy of location and space* (the right to move about in public or semi-public space without being identified, tracked, or monitored), and
7. *privacy of association* (including group privacy); it fosters freedom of speech, including political speech, freedom of worship and other forms of association.

Koops et al. (2017) developed a typology of eight privacy types, four being freedoms from (i.e., right to be let alone), four being freedoms to (self-develop). They also split privacy into four zones: solitude (personal), intimacy (intimate), secrecy (semi-private), inconspicuousness (public zone). They believe every privacy scenario will, to a greater or lesser degree, have an informational element to it. Informational privacy is missing from the list of privacy types in figure 1 because Koops et al. use it as an overlay across all the other eight types. They do this because they want to minimise the risk of neglecting the other types of privacy.

In "The Fourth revolution" Floridi (2014, 129) says that it is common to distinguish four types of privacy, and speaks of these all being "freedoms from" something:

1. Physical privacy (freedom from sensory interference or intrusion)
2. Mental privacy (freedom from psychological interference or intrusion)
3. Decisional privacy (freedom from procedural interference or intrusion)
4. Informational privacy (freedom from epistemic interference or intrusion achieved through a restriction on unknown or unknowable facts about an individual)

There will always be an ongoing need to refine and adapt any typology of privacy in view of societal and technological changes. Finn et al. (2013, 21) say "privacy is a fluid and dynamic concept that has developed alongside technological and social changes." Floridi (2014, 137) similarly acknowledges that the friction in the infosphere is importantly affected by technological innovations and social developments.

Vedder (2004) suggests a new category of privacy distinct from individual or collective privacy called *categorical privacy*. This is a reaction to the ease with which individuals can become associated with new groups as new technologies like data mining emerge. Sigmund (2017) points out that categorical privacy removes just one problem of the privacy concept, but that many others remain.

The above review of privacy types reflects the complex nature of privacy as a concept and helps make the case for a holistic approach to privacy, even if that is fiendishly difficult.

What is an Appropriate Theoretical Framework for Informational Privacy?

Over 50 privacy theories were reviewed. Noteworthy theories include:

- Neil Richards' theory of intellectual privacy is highly relevant to the work of information professionals, comprising freedom of thought, the "right to read," and the right to communicate in confidence (Richards 2015).
- Sandra Petronio's communications privacy management theory is a highly developed rule-based theory based around the idea of negotiated boundaries between the personal data that people choose to conceal and that which they are prepared to share with particular confidants (Petronio and Altman 2002)
- Helen Nissenbaum argues that privacy is best understood through a notion of "contextual integrity," where it is not the sharing of information that is the problem, but the sharing of information outside of socially agreed contextual boundaries. She proposes her "Framework of contextual integrity" (FCI) for analysis of potentially privacy-invading services and practices (Nissenbaum 2010) consisting of five key components (contexts, informational norms, actors, attributes, and transmission principles)
- Floridi's privacy theory forms part of his philosophy of information, and includes the concept of ontological frictions (Floridi 2006a). His theory is information- or data-centric.

Floridi (2008, 199) sees his theory as providing a minimalist, common framework that can support dialogue. He identifies four privacy types, of which informational privacy is the most important one; presenting them all as "freedoms from." Of all the privacy theories reviewed, we believe Floridi provides the best overall theoretical framework, but with some reservations. Firstly, to acknowledge the importance of the full range of privacy types we believe Floridi's privacy theory should be combined with the typology of privacy produced by Koops et al. (2017), who recognise eight privacy types with informational privacy as an overlay across all of them. They also split these privacy types into four "freedoms from" and four "freedoms to," thereby acknowledging the importance of privacy in giving people the freedom to develop. Many aspects of privacy are not fully fleshed out in Floridi's minimalist theoretical framework; but precisely because of this the theory is flexible enough to cope with continually changing technological and social developments that directly impact upon privacy norms.

Tavani (2008) criticises Floridi's privacy theory on two grounds, the first of which supports our contention that Floridi's theory needs to be combined with one that acknowledges the range of privacy types over and above informational privacy. He says that an adequate privacy theory should be able to differentiate informational privacy from other kinds of privacy, including psychological privacy; and distinguish between descriptive and normative aspects of informational privacy in a way that differentiates a (mere) loss of privacy from a violation of privacy.

Floridi's privacy theory appeals for a number of reasons:

- He anchors privacy around human dignity, not ownership or control.
- His theory of ontological friction is a useful way of conceptualizing key issues in informational privacy: flows, movements, and data transfers; processing and use of data; safeguards, etc.
- He considers informational privacy to be the most important type of privacy.
- He treats whole groups as individuals. This modification of the level of abstraction acknowledges that some groups are holders of rights (Floridi 2017a, 83). Big data is more likely to treat types (of customers, users, citizens, demographic population, etc.) rather than tokens (you, Alice, me . . .), and hence groups rather than individuals. The debate between tokens and types is one between nominalism and realism (Floridi 2017a, 85).
- He recognises the revolutionary impact of digital technologies : "ICT's are more redrawing rather than erasing the boundaries of informational privacy" (Floridi 2013b, 230).
- It is the theory best suited to current and emerging challenges posed by developments such as big data, artificial intelligence, algorithms, and machine learning.
- He recognises the importance of data ethics, a new branch of ethics which shifts the level of abstraction of ethical enquiries from being information-centric to being data-centric (Floridi and Taddeo 2016, 1).

Spreadsheet	Conceptual model
Entity type Stakeholders Legal status Organisational attitude to privacy	Entities (individuals, groups, society)
Content (Personally identifiable information, sensitive personal data, demographically identifiable information)	Types of data
Ownership, access and control Public/private	Ownership, access and control
Ontological frictions Information behaviour Digital literacy	Ontological frictions
Purpose of processing Uses	Processing & use
Risks and harms Intent/outcome	Risks & harms
Remedies	Remedies
Rights of data subjects Duties of data controllers	Values, rights and freedoms

Figure 2. Development of the conceptual model mapping the information privacy landscape

What Is a Useful Conceptual Model for Informational Privacy?

During the research, three conceptual models have been developed. One maps the informational privacy landscape and includes a component covering ontological frictions (figure 5). A second model identifies ten types of ontological friction (figure 8). A third conceptual model was developed to address the privacy impacts of library technologies (figure 9).

A literature review was undertaken to understand the nature of informational privacy. This was used to help map out the informational privacy landscape in spreadsheet form, and this was further developed into a conceptual model (see figures 2 and 3). A number of key concepts were identified, and more detail was provided for each of the concepts that had been identified, although there isn't the space to include the more granular information in this article.

A key component of the model are entities. Informational privacy relates to the personal information of identifiable individuals, but the concept of entities was used more widely. For example, it includes library vendors processing personal data. Those companies fall under "groups."

Koops et al. (2017, 569) believe that "informational privacy combines both negative freedom (excluding access to information) and positive freedom (informational self-determination)." We believe it is important to acknowledge the positive aspects of privacy—the ways in which privacy provides space within which people have the freedom to develop, to become the people that they want to be rather than concentrating exclusively on the negative aspects of privacy. Writing in Roessler and Mokrosinska (2015, 79), Solove says that part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocating, and it might not be a place in which most of us would want to live. When protecting individual rights, we as a society decide to hold back in order to receive the benefits of creating the kinds of free zones for individuals to flourish.

Thematic Analysis

To further develop the conceptual model (figure 3) mapping out the informational privacy landscape, a thematic analysis was undertaken. Three pieces of data protection legislation were identified:

- the 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Council of Europe 1981)

- the 1995 Data Protection Directive (EU Directive 95/46/EC 1995) and
- the 2016 General Data Protection Regulation (European Union 2016)

The Convention was chosen because it is the first binding international instrument to set standards for the protection of individuals' personal data; while the two pieces of EU legislation were chosen because "the EU's data protection laws have long been regarded as a gold standard all over the world" (European Data Protection Supervisor 2017).

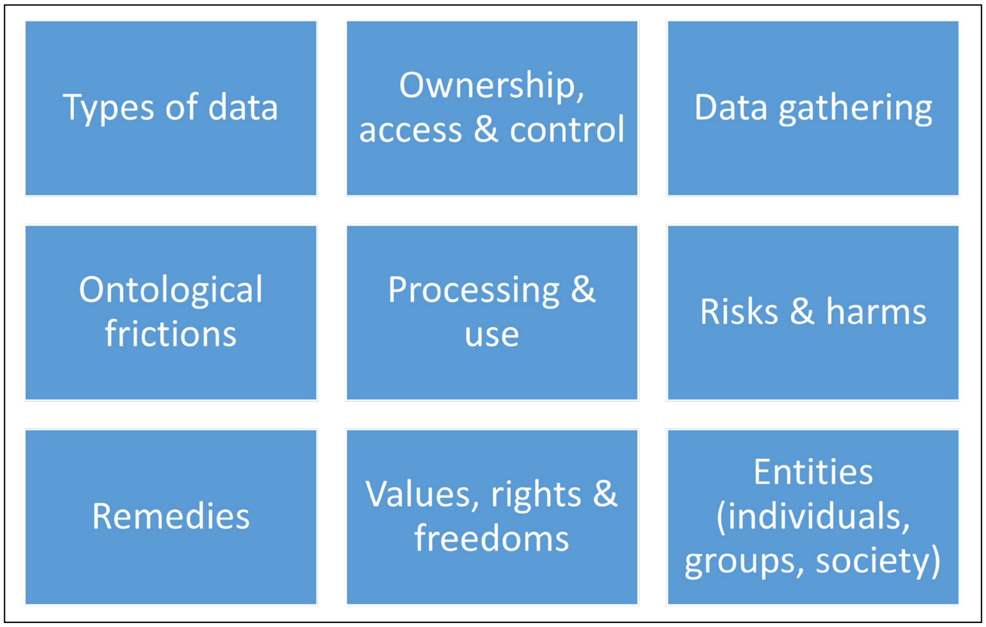
Types of data
Ownership, access & control
Data gathering
Ontological frictions
Processing & use
Risks & harms
Remedies
Values, rights & freedoms
Entities (individuals, groups, society)

Figure 3. Original version of the conceptual model

Across how many of the legislative texts?	Entities	Flow	Other topics	Totals
1	66	39	64	169
2	54	23	62	139
3	30	4	27	61
TOTAL	150 (41%)	66 (18%)	153 (41%)	369

Figure 4. Breakdown of terms identified by broad category, and by how many of the texts they appear in

The approach outlined by Braun and Clarke (2006, 79) was used to undertake the thematic analysis. They say that thematic analysis is a method for identifying, analysing, and reporting patterns (themes) within data. They break down the process of undertaking such an analysis into six distinct phases:

1. Familiarizing yourself with the data
2. Generating initial codes
3. Searching for themes
4. Reviewing themes
5. Defining and naming themes
6. Producing the report

Coding the three pieces of data protection legislation identified 369 words or phrases. It was only practicable to allocate primary codes to each of them, whereas some could have slotted into multiple headings. The 369 words and phrases were categorized into 15 broad themes, which were eventually grouped into three categories.

Entities

1. Natural persons
2. Groups
3. Society
4. Data protection role/function

Flows

1. Borders and frontiers
2. Flows, movements, and transfers
3. Enablers of data flow
4. Obstacles to data flow

Other Themes

1. Power and control
2. Safeguards
3. Values, rights, and freedoms
4. Access

5. Technology
6. National/international
7. Processing of data

Of the 369 words and phrases identified, 61 of them appear in all three pieces of legislation.

As a result of the findings of the thematic analysis, the model mapping the information privacy landscape was expanded to cover three new areas:

- Safeguards
- National/international perspective and territorial scope
- Data flows

The "Entities" were expanded to cover data protection roles and functions; while "groups and institutions" were split into six sub-categories: companies and institutions, groups of individuals, specific categories (such as "health professional" or "interpreters"), states and parties (such as "European Parliament," "Non-contracting states"), legal status, and other groups.

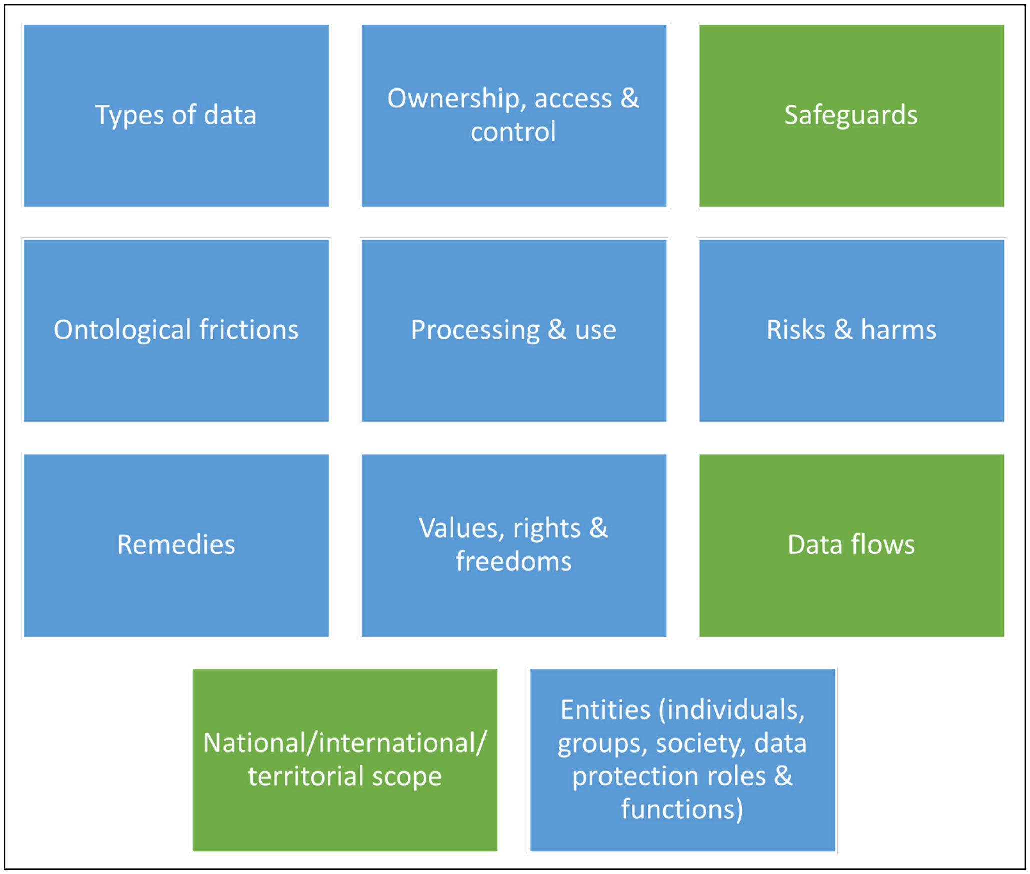
Types of data
Ownership, access & control
Safeguards
Ontological frictions
Processing & use
Risks & harms
Remedies
Values, rights & freedoms
Data flows
National/international/ territorial scope
Entities (individuals, groups, society, data protection roles & functions)

Figure 5. Updated conceptual model following the thematic analysis

We received feedback on the model suggesting that safeguards could form part of the remedies component. However our model envisages remedies as covering judicial remedies to address failures to protect personal data which have already taken place such as compensation, damages, costs, or complaints procedures whereas the safeguards component covers built in protections to prevent those failures from occurring. They can be clustered into:

- References to protect(ions): "Safeguard," "Protect," "Protection of legal persons," "High level of protection"
- Emphasizing compliance: "legal requirement," "comply," "authorized"
- Qualifiers: "shall apply," "shall take," "shall provide"
- Specific requirements: "informed," "relevant," "fairly," "transparency," "explicit consent"

Another piece of feedback suggested merging data gathering and data flow into a single component. The rationale for the data gathering heading was to cover the legal acquisition of data. It covers the question of whether consent is one time, unambiguous, or implied; and whether the data subject was fully aware, partially aware or totally unaware that the data was being gathered. Rather than merging "data gathering" with "data flows," we opted to incorporate data gathering into the "safeguards" component.

The "values, rights and freedoms" component incorporates concepts of democracy, freedoms, human rights, liberty, peace, and respect as well as rights such as the right to rectification and erasure; the right not to be subject to automated decision-making; the right to object to processing; the right to information; the right of access; the right to restrict processing; and the right to data portability. This component intersects, to some extent, with other components. For example, it incorporates the *right* to remedy, whereas the "Remedies" component covers the range

Our model mapping the information privacy landscape	Daniel Solove's infographic on the GDPR
National / international / territorial scope	Territorial scope
Entities (individuals, groups, institutions, society, data protection roles & functions)	The players
Types of data	Personal data Sensitive personal data
Processing and use	Lawful processing
Safeguards	Responsibilities of data controllers and processors
Ownership, access and control	Consent
Values, rights and freedoms	Rights of data subjects
Remedies	Enforcement Data breach notification
Data flows	International data transfer
The following do not appear in Solove's infographic	**Why I included them**
Ontological frictions	Phrase used by Floridi (2005) for the forces that oppose the information flow within (a region of) the infosphere, and hence (as a coefficient) to the amount of work and efforts required for a certain kind of agent to obtain, filter and/or block information (also, but not only) about other agents in a given environment
Risks and harms	Article 29 Data Protection,Working Party 2017, Centre for Information Policy Leadership 2016; Richards and Hartzog 2015

Figure 6. comparison of Solove's GDPR infographic with our map of the information privacy landscape

of available remedies. The National/international/territorial scope component covers issues of jurisdiction but also covers other aspects such as international cooperation between supervisory authorities. One piece of feedback noted how territorial scope can be viewed in terms of the *right* for your personal data not to be transferred to territories that do not offer the same protections as the European Economic Area.

To test the validity of our model mapping the information privacy landscape, we cross-checked it with an infographic setting out the key elements of the GDPR (Solove 2017). Solove is a law professor with an international reputation for his academic work on privacy. Our model is not exclusively focussed on the GDPR, but it is nevertheless useful to compare the two models. Both models have eleven elements, although in a few cases several of Solove's components fit within one of our headings. Two of our elements have no direct equivalents in Solove's infographic, namely ontological frictions and risks and harms.

How Can a Conceptual Model be Used to Investigate Specific Issues of Library Privacy?

For each privacy scenario, there will be several key elements:

"Entities" covers library staff as well as individual library users or citizens. Information professionals advise companies and institutions on compliance and accountability as well as playing a crucial role in protecting the privacy of their users. That role includes providing education and advice on privacy-related issues.

Within "groups" will be companies and institutions. This will include the library's host organisation as well as the vendor companies supplying products and services to libraries, who rely on external companies to deliver the range of library and information services that they provide.

The state in the form of government, the security services, and so on can be seen as an institution through which society makes and enforces its public policies.

All library privacy scenarios will have an informational privacy component. Koops et al. (2017) believe that this can be seen as a derivative or added layer of, or perhaps a precondition to, other forms of privacy; and it is therefore important to be able to acknowledge the other privacy types that are involved in any given library-related privacy situation.

Entities	Privacy Types	Ontological Frictions
Individuals	Bodily privacy	Technological
Groups	Spatial privacy	Social
Society	Communicational privacy	Regulatory
	Proprietary privacy	Sensory
	Intellectual privacy	Spatial
	Decisional privacy	Information behaviour
	Associational privacy	Temporal
	Behavioural privacy	Training & awareness
	Informational privacy	Obscurity
		Contextual

Figure 7. Key elements for privacy scenarios: entities, privacy types, & ontological frictions

Ontological Frictions as a Means of Controlling the Flow of Personal Data

Floridi (2006a) uses the term "ontological friction" to refer to the forces that oppose the flow of information within a region of the informational environment, the "infosphere" as Floridi calls it. It is a useful way of conceptualizing key issues in informational privacy: flows, movements, and data transfers.

Given some amount of personal information available in a region of the infosphere, any increase or decrease in the level of informational friction will affect privacy: the lower the level of informational friction, the higher the accessibility to personal information about the agents will be and vice versa.

There is a limited amount of literature about ontological friction:

- Floridi (2006a) provides an outline of the ontological interpretation of informational privacy based on information ethics. This interpretation stresses that informational privacy is also a matter of construction of one's own informational identity.
- Floridi's ontological theory of informational privacy uses concepts such as ontological friction to interpret informational privacy. Barn et al. (2015) re-cast the theory in terms of modelling constructs and then applies the theory in the form of a Bayesian network of beliefs in the context of a research project aimed at developing a socio-technical system delivered as a mobile app in the UK youth justice system. They use a modelling language to provide a representation suitable for consumption by software engineers so that it can be used as a way of evaluating information privacy concerns in the design process.
- Bates (2018) further develops Paul Edwards' concept of "data friction" by examining the socio-material forces shaping data movements in the cases of research data and online communications data. He articulate a politics of data friction, identifying the interrelated infrastructural, socio-cultural and regulatory dynamics of data friction, and how these contribute to the constitution of social relations. Casanovas (2014) considers ontological friction in the context of Floridi's information ethics.
- Hildebrandt (2011) discusses the "inference problem" whereby the emerging infosphere seems capable of anticipating our behaviours before we become aware of them. She believes such inferences could dissolve the "ontological friction" that safeguards our privacy. The notion of ontological friction is pivotal for an adequate understanding of privacy because it does not start from individual users that control "their" information, but from an infosphere that has as an affordance a measure of opacity of individual citizens.
- McGeveran (2013) discusses frictionless sharing which discloses an individuals' activities automatically rather than waiting for them to authorize a particular disclosure. He does not think a law of friction would address every situation, and he asks whether such a law should be enforced by government or a voluntary design guideline. His article does not cite Floridi.

Pagallo (2010) stresses the impact of digital technologies on ontological friction. He believes that the ontological degree of friction set by P2P systems creates risks and threats for national security, copyright interests, as well as privacy (protection of the personal sphere from unwanted scrutiny).

- Taddeo and Vaccaro (2011) examine a criterion for the ethical assessment of P2P network implementations. They note that the absence of informational friction

> does not depend on the type of information transmitted but solely on the way in which the information is produced, transmitted, and stored.

Other articles include Floridi (2013b; 2017b; 2014), Gutwirth et al. (2014), Martin (2011), Primiero (2016), Primiero et al. (2017), and Strikwerda (2010). These items were scanned for any mentions of potential friction types. In addition, material from the much broader literature review was trawled for factors which could be considered to represent ontological frictions, even if the sources used made no mention of either the phrase "informational frictions" or "ontological frictions." Ten types of friction were found, and these were developed into a conceptual model.

Floridi does not give us a systematic list of friction types. In "The Fourth Revolution" (2014), however, he does provide a few examples of what might affect the informational gap (which he describes as a function of the degree of accessibility of personal data where the larger the gap, the lower the degree of accessibility to personal data). Using the examples given by Floridi, one can identify the following seven friction types:

1. *Sensory*: if the students have excellent hearing, (104); if the students have perfect sight, p. 104.
2. *Spatial*: whether the students have their own rooms (103).
3. *Temporal*: Floridi refers to a science fiction scenario regarding time, and to a device called a chronoscope, p. 104. Floridi says that because of their "data superconductivity," ICTs are well-known for being among the most influential factors that affect the ontological friction in the infosphere (2006b, 110).
4. *Technological*: Floridi says that ICT's "unquestionably and influentially affect informational friction" (105).
5. *Regulatory*: "solutions to the problem of protecting informational privacy can be not only self-regulatory and legislative but also technological" (139).
6. *Contextual* (Floridi discusses several contextual issues, e.g., social contexts (132), and public contexts (141), but the primary reason for identifying contextual frictions as one of the friction types is Nissenbaum's framework of contextual integrity (Nissenbaum 2010).
7. *Social* (Floridi acknowledges that many factors can affect the ontological friction in the infosphere "including, most importantly, technological innovations and social developments" (2014, 137). These are not mutually exclusive, because the social environment is itself increasingly dependent on technology. Floridi gives massive inurbation as an example of social frictions: the abandonment of rural areas in favour of a metropolis (2013b, 235).

In addition to the frictions inspired by Floridi's writings, a further three friction types were identified from other academics and their writings on privacy:

1. *Obscurity* encompasses online obscurity, practical obscurity, and obfuscation. Hartzog and Selinger (2013) explores obscurity, the idea that when information is hard to obtain or understand it is sometimes safe. Obscurity does not mean inaccessible, rather the deterrent is the need for greater effort to get to the data. Selinger and Hartzog (2014) provide examples of why the lack of obscurity can be problematic, how privacy norms can change quickly, and how changes to social norms can quickly change the privacy landscape thereby giving rise to new breaches of etiquette, new privacy interests, and new privacy harms. In view of the way in which computers never forget, Bishop et al. (2013) consider a number of technical approaches to forgetting without deleting. However, these techniques make uncovering the truth harder and more expensive as well as presupposing that individuals have access to the appropriate economic, political, and technological resources.
2. *Information behaviour* is a type of friction because people make a calculated risk assessment as to whether to share information. Dinev and Hart (2006) attempt to better understand the delicate balance between privacy risk beliefs and confidence and enticement beliefs that influence the intention to provide personal information necessary to conduct transactions. They have produced a privacy calculus model to better understand how individuals develop privacy concerns and what consequences these perceptions have in influencing interactions with other individuals, groups, agencies, and vendors. Peoples' behavior changes when they know or when they think that they are being watched—the chilling effect. Penney (2016) undertook an empirical legal study which identified a correlation between online government surveillance and a reduction in traffic to privacy-sensitive Wikipedia articles. PEN America examined how NSA surveillance drives American authors to self-censor, making the point that "we will never know what books or articles may have been written that would have shaped the world's thinking on a particular topic

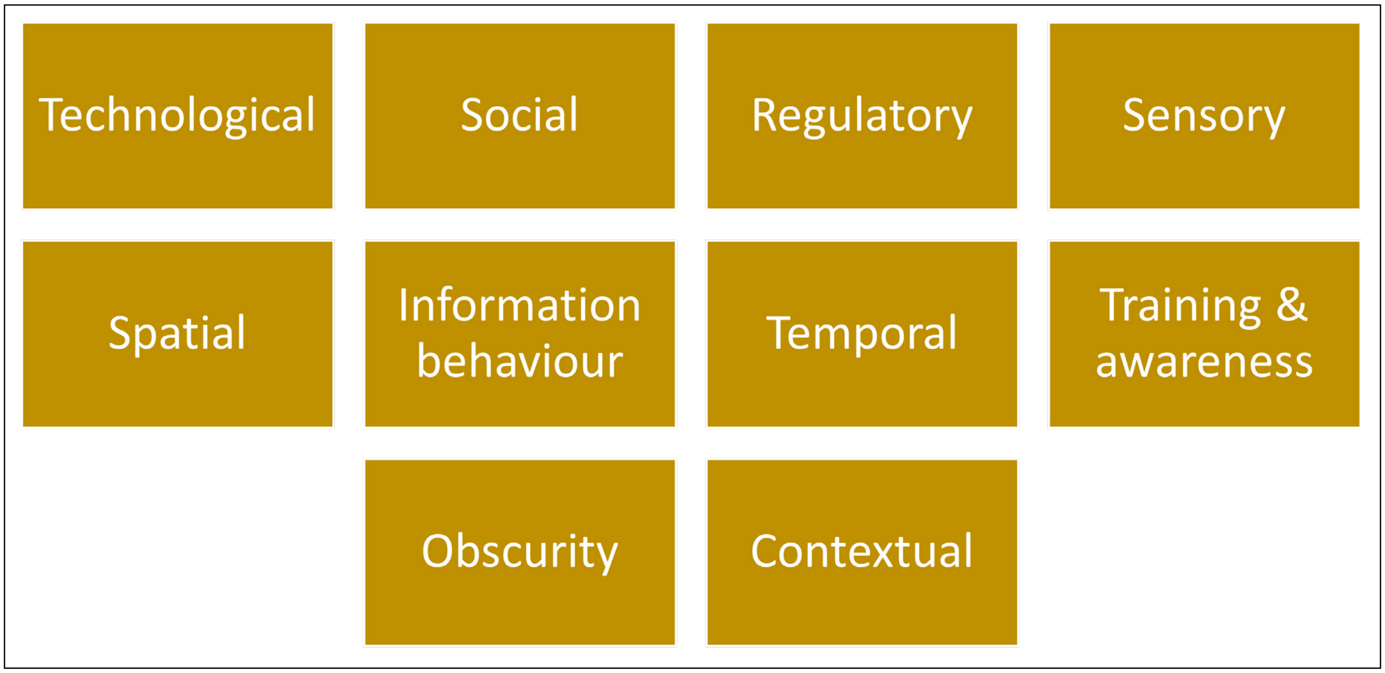

Figure 8. Ontological frictions

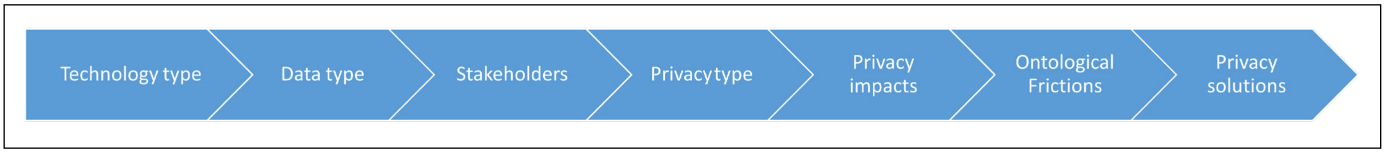

Figure 9. Privacy impacts of library technology

if they are not written because potential authors are afraid that their work would invite retribution" (PEN America 2013, 7).

3. *Training & awareness*: the difference that digital literacy training for library users (including safe online practices) can make, as well as privacy training for librarians. Noh (2014) considers the impact of privacy training on library staff—such as a change in attitude regarding data retention periods, and how the demand for user privacy education increased significantly after the librarian training course had been completed.

Conclusions

The original research question was "How best can we understand informational privacy." It is clear from the work of Koops et al. (2017) that informational privacy is not a privacy type in itself but a derivative layer of other forms of privacy. The corollary of this is that to understand informational privacy one needs to see it in the context of the underlying privacy types to which it relates. Koops et al. (2017) identified eight types: bodily privacy, spatial privacy, communicational privacy, proprietary privacy, intellectual privacy, decisional privacy, associational privacy, or behavioral privacy.

To apply a conceptual model on privacy to a library context, there are three key components that must be considered (figure 7): the entities involved, the types of privacy that are affected, and how the flow of data can be controlled (what Floridi refers to as ontological frictions). We identified ten friction types, seven of which were inspired by Floridi's writings: sensory, spatial, temporal, technological, social, regulatory, and contextual; and a further three were inspired by the writings of other privacy scholars: obscurity, information behaviour, and training and awareness.

The model in figure 9 consists of seven components. The data types, stakeholders/entities, and ontological frictions components build on earlier work from the first conceptual model. The privacy types component brings in the work of (Koops et al. 2017) to acknowledge that each library privacy scenario will affect informational privacy to one degree or another as well as affecting the underlying privacy types to which it relates.

Whilst it is possible to produce provisional lists of technology types, privacy impacts, and privacy solutions, their final composition will depend on the results of the planned Delphi study, questionnaires, and interviews.

References

Abrams, M. 2016. *The Origins of Personal Data and Its Implications for Governance*. Information Accountability Foundation.

Article 29 Data Protection, Working Party. 2017. Guidelines on Data Protection Impact Assessment and Determining Whether Processing is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679.

Barn, B.S., G. Primiero, and R. Barn. 2015. An Approach to Early Evaluation of Informational Privacy Requirements, *Proceedings of the 30th Annual ACM Symposium on Applied Computing 2015*, ACM, 1370-75.

Barron, S. and A. J. Preater. 2018. Critical Systems Librarianship. In *The Politics of Theory and the Practice of Critical Librarianship*. Edited by K. P. Nicholson and M. Seale. Library Juice Press.

Bates, J. 2018. The Politics of Data Friction. *Journal of Documentation* 74(2): 412.

BBC News Online. 2011 Snooping Devices Found in Cheshire Library Computers. *BBC News Online*.

Bishop, M., E. R. Butler, K. Butler, C. Gates, and S. Greenspan. 2013. Forgive and Forget: Return to Obscurity, *Proceedings of the 2013 New Security Paradigms Workshop* 2013, ACM, 1–10.

Blok, P. H. 2002. Het recht op privacy: een onderzoek naar de betekenis van het begrip’privacy’in het Nederlandse en Amerikaanse recht.

Branscomb, A. W. 1985. Property Rights in Information. In*Information Technologies and Social Transformation*. Edited by B. Guile, National Academy Press, 81-120.

Braun, V., and V. Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3(2): 77-101.

British Library. 2016. British Library Annual Report 2015/2016.

Caldwell-Stone, D. 2012. A Digital Dilemma: Ebooks and Users’ Rights. *American Libraries*.

Casanovas, P. 2014. Meaningful Reality: Metalogue with Floridi’s Information Ethics. *Philosophy and Computers* 14(1): 20-25.

Centre for Information Policy Leadership. 2016. Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR CIPL GDPR Interpretation and Implementation.

Clarke, R., 1997. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. *Roger Clarke’s blog*.

Council Of Europe, 1981. *Convention for the Protection of Individuals with Wegard to Automatic Processing of Personal Data*. Council of Europe treaty. Strasbourg, Germany. https://rm.coe.int/1680078b37.

Dinev, T., and Hart, P. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research* 17(1): 61–80.

EU Directive 95/46/EC. 1995. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. *Official Journal of the EC* 23(6).

European Data Protection Supervisor. 2017. The History of the General Data Protection Regulation.

European Union. 2016. Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union,* L119 (May 4).

Finn, R. L., D. Wright and M. Friedewald. 2013. Seven Types of Privacy. In *European Data Protection: Coming of Age*. Edited by S. Gutwerth et al. Springer Netherlands, 3.

Floridi, L., 2005. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology* 7: 185-200.

Floridi, L. 2006a. Informational Privacy and Its Ontological Interpretation. *ACM SIGCAS Computers and Society* 36(1): 1.

Floridi, L. 2006b. Four Challenges for a Theory of Informational Privacy. *Ethics and Information Technology* 8: 109-119.

Floridi, L. 2008. Information Ethics. *Ethics and Onformation Technology* 10(2-3): 189-204.

Floridi, L. 2013. *The Ethics of Information*. Oxford: Oxford University Press.

Floridi, L. 2014. *The 4th Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press.

Floridi, L. 2016. On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology* 29(4): 307-312.

Floridi, L. 2017a. Group Privacy: A Defence and an Interpretation. In *Group Privacy: New Challenges of Data Technologies*. Edited by L. Taylor, L. Floridi, and B. Van Der Sloot. Springer, 83-100.

Floridi, L. 2017b. Group Privacy: A Defence and an Interpretation. In *Group Privacy: New Challenges of Data Technologies*. Edited by L. Taylor, L. Floridi, and B. Van Der Sloot. Cham, Switzerland: Springer International, 83-100.

Floridi, L., and M. Taddeo. 2016. What is Data Ethics? *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences* 374(2083): 1-5.

Gellert, R., and S. Gutwirth. 2013. The Legal Construction of Privacy and Data Protection. *Computer Law & Security Review* 29(5): 522–30.

Gorman, M. 2000. *Our Enduring Values: Librarianship in the 21st Century*. Chicago; London: American Library Association.

Gutwirth, S., R. Gellert, R. Bellanova, M. Friedewald, P. Schutz, D. Wright, E. Mordini, and S. Venier. 2011. Deliverable D1: Legal, Social, Economic and Ethical Conceptualisations of Privacy and Data Protection (Prescient project: privacy and emerging fields of science and technology: towards a common framework for privacy and ethical assessment).

Gutwirth, S., R. Leenes, P. De Hert, and Springerlink Ebook Collection. 2014. *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*. Dordrecht: Springer Netherlands.

Halpin, H. 2018. Library Records of 20 People in Dublin Edited to Include Sexually Explicit Information. thejournal.ie, February 27. https://www.thejournal.ie/data-protection-commissioner-annual-report-3-3874234-Feb2018/.

Hartzog, W., and E. Selinger. 2013. Obscurity: A Better Way to Think about Your Data than "Privacy." *The Atlantic,* January 17.

Hartzog, W., and F. Stutzman. 2013. The Case for Online Obscurity. *California Law Review* 101(1): 1-49.

Hildebrandt, M. 2011. Who Needs Stories If You Can Get the Data? ISPs in the Era of Big Number Crunching. *Philosophy & Technology* 24(4): 371-90.

Kim, D., and Y. Noh. 2014. A Study of Public Library Patron's Understanding of Library Records and Data Privacy. *International Journal of Knowledge Content Development & Technology,* 4(1): 53-78.

Kokott, J., and C. Sobotta. 2013. The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law* 3(4): 222–28.

Koops, B., B. C. Newell, T. Timan, I. Skorvanek, T. Chokrevski, and M. Galic. 2017. A Typology of Privacy. *University of Pennsylvania Journal of International Law* 38(2): 483–575.

Martin, K. E. 2011. TMI (Too Much Information): The Role of Friction and Familiarity in Disclosing Information. *Business & Professional Ethics Journal* 30(1/2): 1-32.

McGeveran, W., 2013. The Law of Friction. *University of Chicago Legal Forum* 1: 15–68.

McLysaght, E. 2011. Data Breach at Trinity College Dublin. *The Journal.ie*, April 29.

Newman, B. L., and B. Tijerna, eds. 2017. *Protecting Patron Privacy: A LITA Guide*. Lanham, MD. Rowman & Littlefield.

Nissenbaum, H. F. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law.

Noh, Y. 2014. Digital Library User Privacy: Changing Librarian Viewpoints through Education. *Library Hi Tech* 32(2): 300–317.

Pagallo, U. 2010. A New "Ring of Gyges" and the Meaning of Invisibility in the Information Revolution. *Journal of Information, Communication and Ethics in Society* 8(4): 364–76.

Pedersen, D. M. 1979. Dimensions of Privacy. *Perceptual and Motor Skills* 48(3_suppl): 1291–97.

Pedersen, D. M. 1997. Psychological Functions of Privacy. *Journal of Environmental Psychology* 17(2): 147–56.

PEN America. 2013. Chilling Effects: NSA Surveillance Drives US Writers to Self-Censor. New York: PEN American Center.

Penney, J. 2016. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal* 31(1): 117–82.

Petronio, S., and I. Altman. 2002. *Boundaries of Privacy.* Albany: State University of New York Press.

Primiero, G. 2016. Designing Systems with Privacy: Formal and Experimental Methods (Powerpoint presentation, Department of Computer Science, Middlesex University, London, May 5). https://schiaffonati.faculty.polimi.it/TFI/lecture%202%20primiero.pdf.

Primiero, G., L. Athiappan, F. Raimondi, and B. S. Barn. 2017. A Tool for Assessing Privacy Awareness in Social Networks. 1–17.

Richards, N. M., and W. Hartzog. 2015. Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review* 19(3): 431–72.

Richards, N. 2015. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford: Oxford University Press.

Roessler, B., and D. Mokrosinska. 2015. *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge: Cambridge University Press.

Selinger, E., and W. Hartzog. 2014. Obscurity and Privacy. In *Routledge Companion to the Philosophy of Technology*. Edited by J. Pitt and A. Shew (Milton Park, UK: Routledge), 1–20.

Sigmund, T. 2017. Ambiguous Character of Information Privacy and Its Possible Solution. *Journal of Information Ethics* 26(2): 34–53.

Solove, D. 2017. The GDPR Summarized in Whiteboard Form. Teach Privacy. https://teachprivacy.com/gdpr-whiteboard/.

Strikwerda, L. 2010. Information Privacy, the Right to Receive Information and (Mobile) ICTs. *Etikk i Praksis: Nordic Journal of Applied Ethics* 4(2): 27–40.

Taddeo, M., and A. Vaccaro. 2011. Analyzing Peer-to-Peer Technology using Information Ethics. *The Information Society* 27(2): 105–12.

Tavani, H. T. 2008. Floridi's Ontological Theory of Informational Privacy: Some Implications and Challenges. *Ethics and Information Technology* 10(2–3): 155.

Vedder, A. H. 2004. KDD Privacy Individuality and Fairness. In *Readings in Cyberethics*. Edited by R. A. Spinello and H. T. Tavani, 462–70. Burlington, MA: Jones & Bartlett Learning.

Westin, A. F. 1967. *Privacy and Freedom*, 1st ed. New York: Atheneum.

Wright, D., and C. Raab. 2014. Privacy Principles, Risks and Harms. *International Review of Law, Computers & Technology* 28(3): 277–98.