Received: 27 August 2019 | Revised: 25 March 2020 | Accepted: 15 April 2020

DOI: 10.1002/asi.24367

RESEARCH ARTICLE

JASIST WILEY

# "The dearest of our possessions": Applying Floridi's information privacy concept in models of information behavior and information literacy

**David Bawden** | **Lyn Robinson**

Centre for Information Science, City, University of London, London, UK

**Correspondence**
David Bawden, Centre for Information Science, City, University of London, Northampton Square, London, EC1V 0HB, UK.
Email: d.bawden@city.ac.uk

**Abstract**

This conceptual article argues for the value of an approach to privacy in the digital information environment informed by Luciano Floridi's philosophy of information and information ethics. This approach involves achieving informational privacy, through the features of anonymity and obscurity, through an optimal balance of ontological frictions. This approach may be used to modify models for information behavior and for information literacy, giving them a fuller and more effective coverage of privacy issues in the infosphere. For information behavior, the Information Seeking and Communication Model and the Information Grounds conception are most appropriate for this purpose. For information literacy, the metaliteracy model, using a modification a privacy literacy framework, is most suitable.

## 1 | INTRODUCTION

The protection of individual privacy has long been recognized as an important issue (DeCew, 2018; Wacks, 2015), Virginia Woolf suggesting that our private life is "infinitely the dearest of our possessions" (Woolf, 2002, p. 58). In suggesting that privacy is of such importance, Woolf may seem to exaggerate. But when we consider that Luciano Floridi has denoted the protection of privacy as "one of the defining issues of our hyperhistorical time" (Floridi, 2014, p. 102) and holds that personal identity itself is not possible without information privacy (Floridi, 2006, p. 111), and that Wu, Vitak, and Zimmer (2019, p. 1) have noted it as "a central issue of the information age [due to] the intertwining relationship between information technology and privacy," perhaps she was prescient. There is also in Woolf's essay an element of prescription; privacy is not necessarily the most important thing for all people, but it should be. Here, there is a glimpse of a very modern attitude, espoused by those such as Akiko Busch (2019) who urges the merits of anonymity and obscurity.

Issues of informational privacy are recognized as of increased importance with the advent of digital information, whose technologies offer, alongside positive affordances, opportunities for privacy harms. This was set out by Salton, who, four decade ago, identified the "obvious and fundamental conflict between society's need for information of many kinds and the individual's right to privacy protection" (Salton, 1980, p. 76).

To preserve privacy, while allowing open and efficient access to information and data requires an understanding of the nature of privacy, a complex and contested concept, whose very nature changes as digital technologies become the norm. In this article, we apply the privacy concepts integral to Luciano Floridi's philosophy of information and information ethics (Floridi, 2013, 2014) to models of information behavior and information literacy.

In particular, the point on which our argument relies is Floridi's perspective that human beings are essentially constituted by their information, and that human nature is a matter of informational patterns.

## 2 | A FLORIDIAN APPROACH TO INFORMATIONAL PRIVACY

We now introduce an approach to privacy based on this Floridian perspective, using six subheadings: the concept of privacy; an overarching philosophical and ethical system; an ontology of information; types of privacy; influence of digital technologies; and informational frictions. Finally, in this section, we offer a series of vignettes to illustrate the differences that arise from this approach compared with other conceptions of privacy. The reader may find it helpful to refer to Table 1 to see how these elements fit together.

### 2.1 | The concept of privacy

Privacy may seem to be an intuitively simple concept, regarded in common sense terms as a "right to be let alone" (Warren & Brandeis, 1890) or "the right of the individual to decide what information about himself should be communicated to others and under what condition" (Westin, 1967, p. 10), but in reality it is highly complex: "The term 'privacy' is used frequently in ordinary language, as well as in philosophical, political and legal discussion, yet there is no single definition or analysis of meaning of the term." (DeCew, 2018, p. 1). As Vasalou, Joinson, and Houghton (2015, p. 918) put it, the concept of privacy is "inherently difficult to reduce to a single definition that is rich enough to explain perceptions and behaviors across a range of contexts. Moreover, recent sociotechnical developments add to the intrinsic complexity between information, physicality, and expression, and as a consequence constantly change the meaning of privacy." Studies of the concept in a variety of disciplines have produced many definitions, concepts, frameworks, and models, some of which have clear relevance for information science; see Bawden and Robinson (2019), Mai (2016, 2019), Rønn and Søe (2019), and Wu et al. (2019) for recent reviews. Some relevant categories and typologies of privacy of direct relevance to our theme are discussed later.

### 2.2 | An overarching philosophical and ethical system

There may be a place for empirically grounded and pragmatic understandings of privacy for particular purposes; Solove (2008) has argued for the value of just such a problem-based approach. However, there are advantages to seeking an understanding rooted in an ethical perspective, which may provide both context and justification for ideas of privacy, relating them to other relevant issues, and also a way of providing an analytical and formal framework for concept development. Rubel and Biava (2014) describe such an approach, using the method of "broad reflective equilibrium," due to Rawls (1999). This is a process of working back and forth, considering particular instances and cases, as well as general principles, and seeking to find a coherent viewpoint, such that the final concepts are consistent and self-supporting (Daniels, 2018). No single approach is a panacea. As Doty (2001, p. 146) puts it, "...privacy is too important to be left only to the lawyers, jurists, policymakers, and even the philosophers." But a solid conceptual understanding is a good place to start. It may lead to a fully developed formal, objective, quantitative, and verifiable assessment of privacy risks, harms, and solutions; see, for example, the proposals of Barn, Primiero, and Barn (2015).

Floridi has developed a comprehensive philosophical approach to information in all its manifestations, including information ethics (Floridi, 2011, 2013, 2019). This includes a concept of ontological information privacy; see Floridi (2005, 2006, 2016, 2017). Floridi's philosophy of

**TABLE 1** Outline conceptual model for Floridian information privacy

| | | | |
|---|---|---|---|
| 1. Philosophy of information, and information ethics: The ground for the privacy concept | 2. Contexts: Onlife and infosphere; information ontology with types of information; relations between inforgs | 3. Typology of privacy and privacy harms: Information privacy being fundamental | 4. Human dignity: The basis for privacy claims |
| 5. Individuals and groups: Constituted by their information; the entities to which privacy can apply | 6. Anonymity and obscurity: Fundamentals of privacy in the infosphere | 7. Information accessibility, flows, and gaps; informational frictions affecting privacy | 8. Digital technologies: Affecting the nature of privacy harms and their solution |

information has been highly influential, but has also received comment and criticism; see inter alia, Furner (2010, 2017), Brenner (2014), Van der Veer Martens (2017), Wu and Brenner (2017), Gorichanaz et al. (2020), and Bawden and Robinson (2018, 2019, 2020). This amounts to what Floridi describes as a "radical reinterpretation [of privacy], one that takes into account the informational nature of ourselves, and of our interactions as inforgs" (Floridi, 2014, p. 119). We now set out what we consider the major and distinctive aspects of this approach to digital privacy. These are summarized in Table 1, as a simple outline conceptual model with eight elements.

Privacy issues in this model fit within, and draw from, a wider information ethics (Element 1 in the model). Burk (2008) and Stahl (2008) were among the first to assert that considerations of privacy need to be set in a wide and robust framework of ethics and require an equally robust model of exactly what constitutes an individual's personal information; they were also among the first to question whether Floridi's information ethics is sufficiently consistent and robust for the purpose. Subsequent development of the model, and experience of its use in practice, verifies that it is indeed consistent and robust. Buschman (2016) voices concerns about whether any ethics-based privacy model may lead to a focus on a narrow set of individual privacy harms. While this point seems well justified, two features of Floridian privacy—its design for the digital environment, which Buschman identifies as a problem for ethics-based privacy in general, and its emphasis on groups as well as individuals—suggest that it may be exempted from Buschman's concerns.

Tavani (2008a) queried whether Floridi's privacy concept is descriptive (this is how things are), as might be appropriate for an ontological scheme, or normative (this is how things should be), as would be appropriate for a system of virtue ethics (which is where Floridi locates his information ethics). For example, when we say that this model of privacy emphasizes the privacy of groups as much as that of individuals, are we proposing as a fact that group privacy is important, or are we urging that group privacy should be taken seriously. We believe that it is essentially the former, but that facilitates the latter; following the example, we can argue because it follows from the principles of information ethics that group privacy is important, it is incumbent upon those making privacy decisions to take explicit account of group privacy.

One of the claims of Floridi's information ethics is that it is universal, applicable to any situation that may be analyzed in informational terms. This has been queried by critics, following Stahl (2008), who argues that it is unreasonable to expect any system of privacy ethics to be universal and proposes instead a discourse ethics based on Habermas' concepts, which does not recognize universal norms of ethics, including privacy, but rather gives procedures for finding universally acceptable solutions in particular cases. Solove (2008) similarly advocates a pragmatic approach, focusing on solving problems of privacy in specific contexts. Both Nissenbaum (2010, 2011) and Rubel and Biava (2014) also prefer context-sensitive solutions to specific privacy issues: the former based on social norms and the later based on the relations between two people and the particular information, which may be shared between them. Nissenbaum's "framework of contextual integrity" provides a set of conceptual entities relevant to online privacy, including actors (subjects, senders, and recipients), attributes (types of information), and transmission principles (constraints on flow of information), enabling the derivation of a model directly comparable to, or able to be integrated into, established information behavior models; it has been applied by McMenemy (2017) to privacy issues affecting information professionals.

Mai (2019) develops this approach by including the contextual nature of the information itself, in addition to the situation and the relations of the persons with the information, in a model designed for a digital environment, and rooted in the semiotics of communication, rather than an ontology of information. Wu et al. (2019) review a number of applications of contextual privacy theory, and they and Wu (2019) develop a nuanced contextualized approach to informational privacy. It is therefore clear that contextual theories are effective in practice, and the question for a universal scheme such as Floridi's is whether it is hospitable to inclusion of specific contextual factors; we address this point later.

Stahl asserts that Floridi's ethics do not deal with issues that are relevant but not informational; he exemplifies this by the consideration of gender issues in the use of information and communication technologies. Floridi's (2008, 2013) response is that his information ethics and associated privacy formulations are universal in that they allow all such issues to be viewed in informational terms given the correct level of abstraction, and that they are hospitable to being extended to cover different meanings and contexts; the system is complete and closed. This seems convincing and implies that a consistent approach, as near universal as feasible, is desirable, rather than a range of piecemeal solutions, with the potential for inconsistency, conflict, and gaps, however pragmatically valuable each may be.

## 2.3 | An ontology of information

At the heart of this approach, Element 2 of the outline model is an ontology of information, with the implication that all informational entities, including, but by no

means only, people, should be respected and protected, and this gives the basic rationale for privacy (Van der Veer Martens, 2017). This moves the idea of privacy from the individual to the information environment (Floridi's infosphere) in which the individual and their information are participants. There have been long-standing concerns about this, see, inter alia, Tavani (2008a), Stahl (2008, and Capurro (2006, 2008). These concerns include the following: that the nature of privacy is being overcomplicated; that the human subject with its subjective view of the world is being lost in a focus on objective impersonal information; and that, since all informational entities have a moral value, it becomes difficult to deal with conflicting interests with respect to privacy. We suggest, following Floridi (2008, 2013) and Ess (2009), that the last point is easily dealt with; although it is true that all informational entities have a moral value, it is not an equal one, and choices and priorities can be established. The second point appears to be a misunderstanding due to an oversimplified view of Floridi's position, specifically the use of levels of abstraction; there is ample scope for consideration of the subjective personal viewpoint in this model. As to the first objection, if privacy were a simple matter, with simple solutions, there would not have been extensive debates about it; the Floridian model, though not simple, is comprehensive and unified, and allows consideration of specific aspects as needed.

As a consequence of the underlying information ontology, the model regards each person as constituted by their information, so that informational privacy is fundamental, overlaying other types. The idea of a specifically informational privacy is generally held to have been initiated by Westin (1967), who suggested that privacy per se amounts to a claim for self-determination of when, how, and to what extent information about them is communicated to others. This view has been influential, although it has been emphasized by Floridi and also by scholars such as Mai (2016) and Rønn and Søe (2019), that new ideas of information privacy are required for the digital environment.

## 2.4 | Types of privacy

Various typologies of privacy, and privacy harms, have been created. Solove (2005) gives a detailed taxonomy of privacy harms; Tavani (2008b) distinguishes physical, decisional, psychological, and informational privacy, noting that these may overlap; and Koops, Newell, Timan, Škorvánek, and Galič (2017) distinguish nine types of privacy: bodily, intellectual, spatial, decisional, communicational, associational, proprietary, behavioral, and informational. The last is regarded as an extra privacy type, overlapping but coinciding with the others. Floridi (2014) notes that physical, mental, decisional, and informational privacy may be distinguished, but regards informational privacy as central:

> Each of us...is a fragile and very pliable entity, whose life is essentially made of information...only within a philosophy of information that sees human nature as constituted by informational patterns do breaches of privacy have an ontological impact (Floridi, 2016, pp. 310-311).

To commentators such as Tavani (2008a) and Burk (2008) who question whether informational privacy can be distinguished from other forms, and whether Floridian privacy is meant to replace or to complement other privacy theories, Floridi (2008, 2013) argues that the model gives a common framework in which to analyze and contextualize all specific forms of privacy, given that these are necessarily informational in nature. Tavani (2008a) suggests that it could incorporate other insights, such as Nissenbaum's "privacy as contextual integrity." This is a strong argument for Floridi's model, since it appears highly hospitable to, rather than competitive with, contextually-specific privacy models and concepts; see Ess (2009) for an early argument along these lines. Furthermore, the basic concepts within Floridi's model may be used to develop formal contextual models for digital privacy, using concepts of information accessibility, information gap, information flow, and ontological friction; see, for example, Primiero (2016).

In applying Floridi's ideas of privacy, while accepting its central idea that all privacy is essentially informational, we may include other types of privacy, such as those of Tavoni or Koops et al., regarding them as varieties of informational privacy; Element 3 of the outline model. This hospitality enables Floridi's privacy framework to effectively bridge the two approaches to digital privacy most commonly adopted, termed by Mai (2019) the "control approach" and the "access approach." The former identifies privacy with the ability of an individual to control information about themselves, and to place restrictions on who can have access to it; a kind of property right to our own digital information (Tavani, 2008b, Moore (2010). The latter identifies privacy with the idea of having control over our information in all respects, including but going beyond granting access to it. The fact that these two seemingly disparate views of digital privacy may be subsumed within a larger consistent framework is a further argument for adopting a Floridian understanding of privacy.

Fundamental to Floridi's model is the belief that, because personal information plays a crucial constitutive role in who I am and who I can become, protection of privacy should be identified as protection of personal identity and a breach of informational privacy as an aggression against personal identity and self-development. Protection of privacy should be based directly on protection of human dignity, rather than on secondary considerations, such as a right to property, to freedom of expression, or to privacy per se. Human dignity is here a matter of our constantly becoming ourselves, keeping our identity and choices open, building a sense of ourselves and the world (Floridi, 2016); this is reflected in Element 4 of the model.

This is a significant distinction from other digital privacy models, which has two positive consequences: privacy issues may be addressed in a consistent and holistic manner, rather than by ad hoc case-by-case solution; and the concept of privacy is widened, so that the maximum numbers of privacy harms may be addressed. The latter goes some way to allaying the concerns of those, such as Buschman (2016), who worry than an ethics-based privacy model may address too limited a set of privacy harms.

Floridi's approach to privacy holds that that group privacy is as important as individual privacy (Floridi, 2017), reflected in Element 5 of the outline model. While the importance of privacy for groups, particularly marginalized groups, is undeniable, Wu et al. (2019) and Wu et al. (2019) giving examples, and was identified many years ago by Westin (1967), consideration has mainly focused on natural grouping formed by evident criteria: age, gender, ethnicity, educational level, income, and so on. Floridi asserts that any group, including those defined by algorithm, may be just as valid an entity as an individual in the sense of being defined by their information, and hence just as entitled to informational privacy; Mai (2016) also emphasizes this point. Mittelstadt (2017) applies this approach to the protection of privacy for ad hoc groups formed algorithmically from big data analysis, noting that such groups need not conform to intuitively understood groupings, and that Floridi's conception offers advantages over other privacy formulations in dealing with them.

## 2.5 | Influence of digital technologies

Digital technologies can both defend and damage privacy, and these can change understanding of it, by altering two factors: *anonymity*, the unavailability of personal data, due to the difficulty of collecting and processing it; and *obscurity*, where personal information has been collected and is in principle available, but would require undue time and effort to find. These factors are intrinsic to the Floridi approach (Element 6 in the outline model), designed as it is for the digital infosphere, and the "cleaving power" of digital technologies. It is not the only privacy model designed for the digital realm; other examples are those due to Mai (2016, 2019), who presents a "datafication" privacy model relating to big data, and van Hoboken (2019), who analyses the problems caused by the pervasive processing of personal data. However, the demonstrated reach of Floridi's ethics, into areas including big data, information quality, artificial intelligence, cybersecurity, open data, surveillance, and algorithmic inference, gives confidence that it is an appropriate model for the digital environment; see, for example, Arberg (2018), and Barn et al. (2015), as well as numerous papers by Floridi and coauthors. It meets the requirements of Mulligan, Koopman, and Doty (2016), who stipulate that any conceptual model for privacy should be adaptable to changing contexts, particularly technological.

## 2.6 | Informational frictions

Finally, the model recognizes that "Privacy is a function of the informational friction in the infosphere (Element 7 in the model). Any factor increasing or decreasing friction will also affect privacy" (Floridi, 2014, p. 105). The lower the friction, the lower the degree of informational privacy that can be implemented. Informational friction, similarly to Bates' (2018) data friction, refers to all forces opposing free flow of information and data, and to the amount of work needed to access and process information. Examples of such frictions are resources such as computer power and access speeds; physical conditions such as distance, noise and lighting; access issues such as metadata and information architecture; legal issues such as copyright; and user issues such as information literacy. Digital technologies, by altering the nature of informational frictions, can both reinforce and erode informational privacy, as included in the model as Element 8. Informational frictions are typically analyzed conceptually and qualitatively, but are also amenable to formal analysis; see, for example, Walton (2014). Informational privacy is achieved by optimization of frictions, though this emphatically does not simply mean increasing frictions in the hope that this may support privacy. Rather we need a thoughtful treatment of personal information based on a proper analysis of privacy (Floridi, 2014).

## 2.7 | Floridian privacy vignettes

The following three vignettes show ways in which this conception of privacy differs from others: the first is an adaption of an actual incident, the other two are hypothetical.

### 2.7.1 | The charity's app

A charity whose function is to provide support to those suffering emotional distress develops an app that identifies social media posts, which may indicate a possibility of self-harm, and alerts people who have registered to monitor that user; they must follow, and be followed by, the user, indicating that they have a relationship. The charity was surprised by the intensely angry reaction, which led to the app being deactivated within hours. They felt that there were no privacy issues since the posts were on the public timeline and could be seen by anyone; the app did not amend or comment on them, but simply repeated them to other users who might be expected to have seen them anyway; the results for the user could not be harmful, they would be either negligible or highly beneficial; and the other users involved were known to be friends of the user. On the basis of a Floridian model of privacy, the issue is clear: the dignity of the user is infringed by the drawing of unwanted attention to potentially sensitive information, and this is not ameliorated by any other arguments.

### 2.7.2 | Alice's analytics

Alice is a librarian at a university charged with using library analytics to identify opportunities for service improvement. She finds an unusual pattern in the behavior of some patrons, whom she identifies as mainly female students of technology subjects from a particular ethnic background. She believes that she can recommend targeted services to help this group of students. Alice does not see any privacy implications in her suggestion. Although the students concerned will necessarily be identified, their data are being used only for the purpose for which it was collected, the improvement of library services. The students concerned will not be identified to others, and there seems to be no harm in what is proposed; the only impact on this group of students will be an offer of enhanced library services. However, from a Floridian perspective, there are serious privacy concerns. These students are being treated differently, albeit from benevolent motives, because of their membership of an algorithmically determined group, which they did not ask to join, and with which they may not necessarily wish to be associated. This is not an argument against the use of analytics, rather a statement of the necessity to consider the privacy of all groups, included those determined by algorithm.

### 2.7.3 | Bob's creative writing

Bob is a middle-aged, conscientious, and serious-minded financial professional. Bob's employers encourage their staff to make time for creative pursuits, while his family wish that he would do something other than work. Bob, somewhat timidly, takes up creative writing and participates in an online forum, using a *nom de plume*; he wins a forum award for the best newcomer, and the forum inadvertently releases his real name. This is clearly a privacy breach, and the forum managers apologize; however, they feel it is a trivial matter and do not see why Bob would be upset. He has suffered no harm, nor has his reputation been damaged; on the contrary, his family and work colleagues are likely to be pleased that he has taken their advice and to congratulate him on his success. In a Floridian perspective, however, Bob has every right to be offended at a serious privacy harm. He is trying to grow and develop as an individual, and he cannot do so effectively if he is observed, commented on, or even congratulated.

## 3 | A FLORIDIAN PRIVACY MODEL

It is tempting, as we argued in Bawden and Robinson (2019), to develop a conceptual model for privacy, based on Floridi's principles, augmented as necessary by aspects of the other relevant models. We show a simple block diagram as a precursor for such a model in Table 1. In this simple model, the eight elements are essentially independent. Clearly there are some dependencies, as noted in the text; in particular privacy-specific elements 5–8 are strongly influenced by the privacy fundamentals expressed in Elements 3 and 4, in turn influenced by the wider issues of Elements 1 and 2.

Interesting though the further development of such a model might be, given the plethora, of models and frameworks for privacy per se, and equally for information behavior and literacy, two important issues within information science which have an evident relation to privacy, the creation of yet another seems undesirable. To make practical use of the conceptualization discussed earlier, we propose that it is better to try to infuse existing constructs with an explicit Floridian perspective on privacy, augmented by elements of the other models noted above.

In terms of Reynolds' (1971) typology of theory, models of information behavior and information literacy would, depending on their formulation be classed as Type 2 (an interrelated set of definitions, axioms, and propositions) or Type 3 (descriptions of causal processes) (Case & Given, 2016, p. 185; Pinfield, Wakeling, Bawden, & Robinson, 2020). Such models have been formulated from conceptual analysis, from analysis of secondary data, and from empirical data collection. Their primary purpose is to aid understanding of concepts and

processes, although they may serve additional purposes, for example, the design of systems (Makri, Blandford, & Cox, 2008), and of instructional programs (Robinson & Bawden, 2018a, 2018b). The reason for including privacy concepts in such models is therefore both to aid a fuller understanding and to enhance practice.

We consider first the inclusion of privacy concepts in information behavior models, before considering models for information literacy.

## 4 | PRIVACY IN INFORMATION BEHAVIOR MODELS

In terms of Floridi's philosophy of information, as outlined earlier, privacy may be explained in terms of information accessibility within an environment, informational gap, informational (or ontological) friction, and information flow. It seems sensible to seek to incorporate this idea into one or more of the available models for information behavior. (The terms "theories" and "paradigms" are also used to describe some of these, but for simplicity we will use "models" for all.)

Numerous such models and theories have been derived: well-known examples are the family of models due to Wilson, and inter alia those proposed by Ellis, Foster, Kuhlthau, Dervin, Ingwersen and Järvelin, Savolainen, Krikelas, Johnson, and Leckie. These are reviewed by Ford (2015), by Case and Given (2016), and by Robson and Robinson (2013). None specifically address privacy issues, although in some cases it is clear where such issues might be introduced: for example, Wilson's (1999) model includes a section for "channels of communication," where informational frictions would naturally be placed.

A number of models have been proposed from communication theory, focusing on the communicator and the communication channel, rather than the recipient and information seeker. Case and Given (2016, p. 144) denote these as models of "exposure" to mass communication, rather than of pro-active "seeking" for information; see Robson and Robinson (2013) for an assessment of their relevance in information science. Again, issues of privacy are not addressed explicitly, but in some cases it is clear where they could be incorporated. For example, in the model due to Maletzke (1963), the section "pressure or constraint from the [communication] medium" is suitable for the consideration of information and data frictions.

It may be questioned whether it is reasonable to retrospectively inject a privacy element into any model, when this was not included initially. The rationale is that no model for information behavior (or indeed for information literacy) has been claimed to be final and complete; on the contrary, their originators generally state explicitly that they may be extended to accommodate new concepts and contexts. Were this not an acceptable way to proceed, then we would be left with an everincreasing array of static, partial, and outdated models, for which the only remedy would be a continual creation of new models to deal with new technologies and new information environments (Savolainen, 2016, 2019), hardly a desirable situation. Expansion of existing models has been recommended and exemplified over a long period; examples are Robertson (2000) for information retrieval, Walton (2017) for information literacy, and Meho and Tibbo (2003), Makri et al. (2008), Robson and Robinson (2013), Savolainen (2016), and Wilson (2016) for information behavior; Case and Given (2016, pp. 146–147) review some extensions and combinations of information behavior models.

In principle, privacy issues could be introduced into any information behavior model, but in practice some kinds of model seem better suited to this task, and more hospitable to these issues than others. We illustrate this by showing how privacy concerns may be included in both process models and interpretivist paradigms (Case & Given, 2016).

## 5 | FLORIDIAN PRIVACY IN PROCESS MODELS FOR INFORMATION BEHAVIOR

Process, or flowchart, models of information behavior have formed one major strand in the study of information behavior, epitomized by the series of models due to Tom Wilson (Case & Given, 2016; Ford, 2015). To illustrate the incorporation of Floridian privacy ideas into this kind of model, we use the Information Seeking and Communication Model (ISCM) (Robson & Robinson, 2013, 2015). This is an expansion of Wilson's style of model, including insights from several models of this kind, and is intended to combine information seeking, information use, and information communication in one model. The ISCM, in its revised version (Robson & Robinson, 2015), is shown diagrammatically in Figure 1. It is suitable for our purposes in three ways.

First, it is comprehensive in its inclusion of all aspects of the seeking, accessing, communicating, and using of information, rather than focusing only on certain aspects. This means that can potentially deal with all privacy issues and harms.

Second, most process models are derived only from the perspective of the information seeker or user, the recipient of the message (information behavior models), or of the sender or communicator (communication models). Privacy is a two-way issue; we must consider

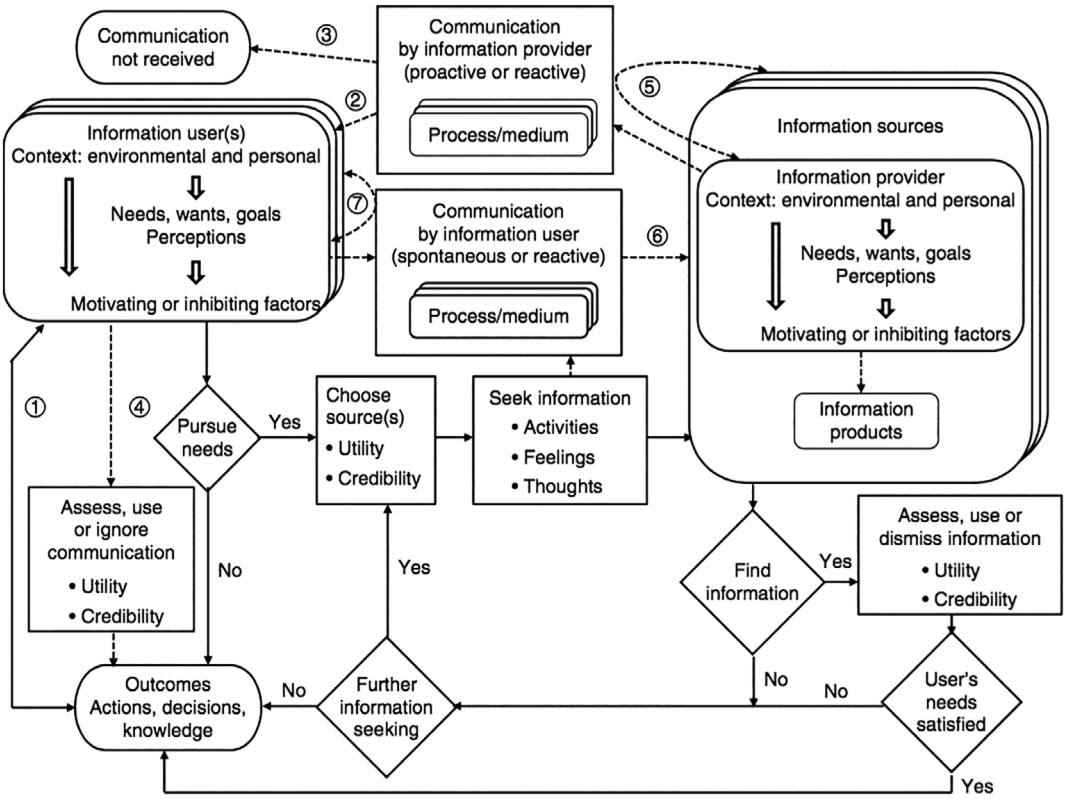


**FIGURE 1** The ISCM model. Reproduced by permission from Robson and Robinson (2015)

both communicator and recipient (Nissenbaum, 2011). The ISCM model, uniquely among the process models for information behavior, is designed to combine the two perspectives (Savolainen, 2016). The two roles are regarded as interchangeable: communicators/providers of information may become recipients/users and vice versa, either within a single information interchange, or over distinct interchanges. Privacy issues may occur at any point, with both parties needing to be aware of potential privacy harms.

Third, while most information behavior models take the perspective of the individual seeker or user, the ISCM is by design broader, focusing on "individuals, groups and organizations" (Robson & Robinson, 2013, p. 185), appropriate for considering groups as well as individuals for privacy purposes. Indeed, a study of the value of the ISCM in understanding the aspects of health care communication focused on two groups as communicators and recipients: medical staff in a UK government agency and in pharmaceutical companies (Robson & Robinson, 2015).

The privacy concepts identified earlier may be incorporated into the ISCM quite straightforwardly, as follows:

- The various ontological frictions are represented within the "communication process and medium" section.
- The "user" and "provider" sections refer to individuals, groups or organizations.
- The "user context" and "provider context" sections, with their "motivating and inhibiting factors," cater for privacy norms and codes; regulations and codes of ethics for pharmaceutical information were included in a study of the application of the ISCM in health care (Robson & Robinson, 2015).
- The "outcomes" section in the ISCM focuses on positive outcomes—actions, decisions, and knowledge—but is equally usable for undesirable outcomes, including privacy harms.

Although these could be entered explicitly into a "privacy version" of the ISCM, we think it better that the model be left as a general one, with privacy concepts recorded as necessary.

## 6 | FLORIDIAN PRIVACY IN INTERPRETIVIST PARADIGMS FOR INFORMATION BEHAVIOR

As our example of this approach to information behavior, from the several widely used models, we take "information grounds," an approach originally derived from the

social constructionist approach of Tuominen and Savolainen (1997), and originally developed by Karen Fisher (Pettigrew) (Fisher, 2005).

An "information ground" is understood as an environment, physical or digital, temporarily created by the behavior of people who have come together to perform a given task, other than communication of information, from which emerges a social atmosphere that fosters the spontaneous exchange and sharing of information. Environments studied as information grounds include foot clinics, shops, restaurants, public transport, skills training sessions, social spaces and waiting rooms of all kinds, and social network sites; see, for example, Pettigrew (1999), Fisher, Durrance, and Hinson (2004), and Fisher, Landry, and Naumer (2008), and Counts and Fisher (2010).

This model has attributes that make it suitable for including privacy concepts. It focuses on groups as well as on individuals, and on a continuous two-way exchange of information, with roles of requestors and providers alternating. Information grounds are necessarily context rich, with conventions, roles, and norms invoked to explain the nature of the information exchanges, and hence naturally hospitable to privacy concerns and potential harms. In a typical information ground, with a relatively small number of participants, known to some degree to each other, both anonymity and obscurity will be significant privacy factors.

The level of perceived privacy was one of the main factors affecting preference for information grounds in a study of college students by Fisher et al. (2008). The preference was not automatically for more privacy:

> Places that include private areas for talking or tables that are far enough away from each other foster conversations that may be personal. Conversely, information grounds might be attractive because they enable eavesdropping, which may contribute to the overall richness of the place.

This is an example of the need for a balance of ontological frictions, in this case audibility, noted earlier. Ambient noise as a characteristic of information grounds is specifically discussed by these authors. This is an example of how informational frictions receive a natural treatment in the information grounds model, as are the comments on the ease of use of mobile phone interfaces in a digital information ground (Counts & Fisher, 2010).

A typical diagrammatic representation of an information ground in shown in Figure 2.

This has the concept of privacy in the "place" facet, effectively restricted to representing the ontological frictions aspect. Other aspects of privacy could be located in the "information" facet, with information flows and information technologies included in the concept of how information is created and shared. In the "people" facet, the concepts of membership type and social type allow for the group privacy aspect, while motivation encompasses individual aspiration for privacy.

Finally, we mention an interpretivist model for slow information behavior, which elucidated the concept of "informational balance," a careful and mindful choice of which sources of information to use, and how and why to consume information (Poirier & Robinson, 2014). Although this study did not deal explicitly with privacy issues, it focused on finding an optimal balance of

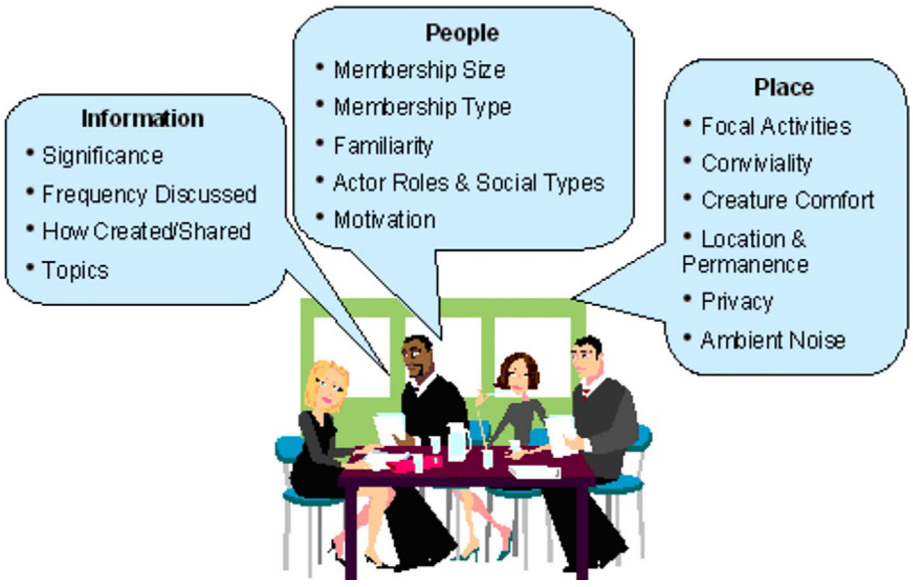


**FIGURE 2** Information grounds. Reproduced by permission from Fisher et al. (2008) [Color figure can be viewed at wileyonlinelibrary.com]

ontological frictions; the speed and ease of access to information, and hence the amount of information processed in a given time. This is another example of the ability of some existing information behavior models to incorporate Floridian privacy concepts with minimal adaptation.

The abovementioned analysis shows that privacy concepts may be included naturally into information behavior models; both those where privacy is an explicit concern in the initial construction of the model (information grounds) and where it is not (ISCM and Slow). This does not mean that privacy concepts should be included in all information behavior models, nor that those which are less amenable to inclusion of privacy issues, are inferior; the latter may be intended for specific issues or contexts, where privacy may not be regarded as an issue worth including. But, given the increasing importance of privacy issues, we might say that models which naturally incorporate these issues are likely to prove more generally applicable and useful.

Having established that Floridian privacy concepts may be included in existing models for information behavior, with relatively little modification, we turn to models for information literacy.

## 7 | INFORMATION LITERACY MODELS

As with information behavior, there are numerous models for information literacy. Again they fall into two general categories, an older style of "competence" models denoting individual skills and competences for problem solving, and newer, more holistic, flexible, and all-embracing "relational" models; for reviews, see, for example, Secker and Coonan (2013), McNicol and Shields (2014), Forster (2017), and Robinson and Bawden (2018a, 2018b).

The earlier models focused strongly on the use of formal information sources for education, and gave little attention to privacy issues. These models generally had components dealing with ethical issues, which are as follows:

- "understand the economic, legal, and social issues surrounding the use of information, and access and use information ethically and legally" [ACRL Standards]
- "gather, use, manage, synthesise and create information and data in an ethical manner" [SCONUL Seven Pillars]
- "the ethical dimension of information" [ANCIL].

However, given the educational focus of these models, these sections tended to be used for issues such as copyright and plagiarism. It is only with the more modern holistic form of model, with an increased emphasis on the digital environment generally, and on social media in particular, that privacy concepts enter explicitly into information literacy promotion.

The only widely known information literacy model that explicitly refers to privacy is metaliteracy (Jacobson & Mackey, 2013; Mackey & Jacobson, 2014). This is a holistic and flexible model, intended to be a comprehensive framework, which unifies information literacy with related literacies, such as media literacy and computer, or digital, literacy, and with an emphasis on open learning, social media and participation, creation, and collaboration.

One of the specifically stated goals of the metaliteracy approach is "understand personal privacy, information ethics and intellectual property issues in changing technology environments." As Jacobson and Mackey (2013, p. 89) point out, this is not a new idea within information literacy, but "its importance has become magnified in today's de-centred information environment. Personal privacy has taken on a new meaning in collaborative social settings when users are willing to share so much information online. At the same time, the ways in which personal privacy can be violated have grown considerably."

The specific inclusion of privacy as a goal suggests that metaliteracy, and similar newer holistic frameworks, may be the best vehicle for introducing Floridian privacy concepts into information literacy models. Their emphasis on flexible adaption to new, and rapidly changing, digital environments is also appropriate, as is their treatment of information literacy as a characteristic of groups, rather than the solely individual focus of the earlier type of model. The focus of earlier models was on information access and use, whereas the newer models focus as much on communication and sharing, providing for consideration of privacy as two-way issue.

However, the open and flexible nature of these models gives little or no prescription as to which specific contexts should be introduced. While they are certainly hospitable to privacy concepts based on a philosophy of information, exactly how these are expressed in such models is left undetermined.

A good indication of how this might be achieved is given by the concept of "privacy literacy," a concept overlapping with, though distinct from information and digital literacy. Privacy literacy was introduced by Rotman (2009), as a framework with five elements, later slightly revised by Wissinger (2017). This framework may be readily adapted to include the Floridian privacy concepts discussed earlier, with the aim of making it more generally applicable to all privacy concerns, beyond the

**TABLE 2** Privacy literacy frameworks

| | Rotman | Wissinger | Floridian |
|---|---|---|---|
| Element 1 | Understanding the characteristics of different facets of information | Understanding how personal information is used online | Understanding the characteristics of information, and how personal information is used onlife; understanding nature and types of privacy |
| Element 2 | Recognizing online social interaction as a venue for potential threats to privacy | Recognizing the various places personal information may be shared online | Recognizing the various places in which, and mechanisms whereby, personal information may be shared onlife; informational frictions |
| Element 3 | Realizing the possible outcome of information disclosed in online social interaction | Realizing the consequences of sharing personal information online | Realizing the consequences of sharing personal information onlife; privacy harms and their solutions |
| Element 4 | Evaluating possible threats to privacy in a given social interaction | Evaluating the risks and benefits of sharing personal information online | Evaluating the risks and benefits of sharing personal information onlife for groups and individuals |
| Element 5 | Deciding how and when to divulge information within the online social interaction | Deciding when to share personal information online | Deciding when and how to share personal information onlife; balancing informational frictions |

social media environment which was the initial focus for privacy literacy. The elements of these three privacy literacy frameworks are compared in Table 2.

The Floridian version involves an understanding of the characteristics both of information and of privacy, setting this understanding in the "onlife" realm, where the online and offline realms merge, adds the specific understanding of ontological frictions, stipulates specific recognition of a range of possible privacy harms, advocates a thoughtful treatment of personal information, and extends this to both individuals and groups, and to the sharing of personal information onlife, implying an explicit understanding of ontological frictions. The concepts that provide the links between this table and the summary model in Figure 1 are as follows: information ontology and ethics; onlife and infosphere; nature, types, and contexts of privacy; privacy of both groups and individuals; and informational frictions.

It therefore seems clear that Floridian concepts of privacy may be readily included in the newer conceptions of information literacy, such as metaliteracy, through the mechanism of a component following the precepts of privacy literacy, with relatively little modification.

## 8 | CONCLUSIONS

It is clear that concepts of informational privacy, drawn from Floridi's philosophy of information, and his information ethics, can be quite readily included in models for information behavior and for information literacy, with the need for extensive modification. In the case of information behavior, two very different models, one from the process model family and one from the class of interpretivist paradigms, were shown to be suitable. In the case of information literacy, an example of the newer type of holistic model, when augmented by a somewhat extended privacy literacy framework, was appropriate. The relative ease, and naturalness, with which Floridian concepts such as anonymity, obscurity, and ontological friction, mesh with existing concepts within these conceptual models of the information sciences indicates that it is indeed reasonable to regard Floridi's philosophy of information as an appropriate theoretical foundation for our discipline (Bawden & Robinson, 2018). More generally, it shows the value of formal and theoretical underpinnings to the models and frameworks of the information sciences.

Future work, building on these ideas, would include a fuller development, and evaluation of these kinds of models in contexts for which privacy is especially important. Evaluation of a more formal analysis of informational privacy of the kind pioneered by Primiero (2016), within such models would also be worthwhile.

## REFERENCES

Arberg, N.L. (2018). *Informational privacy and the internet* (Unpublished master's thesis). University of Copenhagen, Denmark.

Barn, B., Primiero, G. & Barn, R. (2015, April). An approach to early evaluation of informational privacy requirements. *ACM Symposium on Applied Computing*. Salamanca, Spain.

Bates, J. (2018). The politics of data friction. *Journal of Documentation*, *74*(2), 412–429.

Bawden, D., & Robinson, L. (2018). Curating the infosphere: Luciano Floridi's philosophy of information as the foundation for library and information science. *Journal of Documentation*, *74*(1), 2–17.

Bawden, D., & Robinson, L. (2019). "Essentially made of information": Concepts and implications of informational privacy. *Information Research*, *24*(4) paper colis1913. Retrieved from. http://www.informationr.net/ir/24-4/colis/colis1913.html

Bawden, D., & Robinson, L. (2020). Still minding the gap? Reflecting on transitions between concepts of information in varied domains. *Information (Switzerland)*, *11*(2), 71.

Brenner, J. E. (2014). Information: A personal synthesis. *Information*, *5*(1), 134–170.

Burk, D. L. (2008). Information ethics and the law of data representations. *Ethics and Information Technology*, *10*(2–3), 135–147.

Busch, A. (2019). *How to disappear: notes on invisibility in a time of transparency*. New York, NY: Penguin.

Buschman, J. (2016). The structural irrelevance of privacy: A provocation. *Library Quarterly*, *86*(4), 419–433.

Capurro, R. (2006). Towards an ontological foundation of information ethics. *Ethics and Information Technology*, *8*(4), 175–186.

Capurro, R. (2008). On Floridi's metaphysical foundation of information ecology. *Ethics and Information Technology*, *10*(2–3), 167–173.

Case, D. O., & Given, L. M. (2016). *Looking for information: A survey of research on information seeking, need, and behavior* (4th ed.). Bingley: Emerald.

Counts, S., & Fisher, K. E. (2010). Mobile social networking as information ground: A case study. *Library and Information Science Research*, *32*(2), 98–115.

Daniels, N. (2018). Reflective equilibrium. In E. N. Zalta (Ed.). Retrieved from *The Stanford encyclopedia of philosophy (fall 2018 edition)*. Stanford CA: Stanford University. https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=reflective-equilibrium

DeCew, J. (2018). Privacy. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy (spring 2018 edition)*. Stanford, CA: Stanford University. Retrieved from https://plato.stanford.edu/archives/spr2018/entries/privacy

Doty, P. (2001). Digital privacy: Towards a new politics and discursive practice. *Annual Review of Information Science and Technology*, *35*, 115–245.

Ess, C. (2009). Floridi's philosophy of information and information ethics: Current perspectives, future directions. *The Information Society*, *25*(3), 159–168.

Fisher, K. E. (2005). Information grounds. In K. E. Fisher, S. Erdelez, & L. E. F. McKechnie (Eds.), *Theories of information behavior* (pp. 185–190). Medford NJ: Information Today.

Fisher, K. E., Durrance, J. C., & Hinson, M. B. (2004). Information grounds and the use of needs-based services by immigrants in Queens NY: A context-based outcomes evaluation approach. *Journal of the American Society for Information Science and Technology*, *55*(8), 754–766.

Fisher, K. E., Landry, C. F., & Naumer, C. (2008). Social spaces, casual interactions, meaningful exchanges: "information ground" characteristics based on the college student experience. *Information Research*, *12*(2), 291. Retrieved from. http://informationr.net/ir/12-2/paper291.html

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology*, *7*(4), 185–200.

Floridi, L. (2006). Four challenges for a theory of informational privacy. *Ethics and Information Technology*, *8*(3), 109–119.

Floridi, L. (2008). Information ethics: A reappraisal. *Ethics and Information Technology*, *10*(2–3), 189–204.

Floridi, L. (2011). *The philosophy of information*. Oxford: Oxford University Press.

Floridi, L. (2013). *The ethics of information*. Oxford: Oxford University Press.

Floridi, L. (2014). *The fourth revolution: How the infosphere is shaping human reality*. Oxford: Oxford University Press.

Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy and Technology*, *29*(4), 307–312.

Floridi, L. (2017). Group privacy: A defence and an interpretation. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group privacy: New challenges of data technologies* (pp. 83–100). Cham: Springer.

Floridi, L. (2019). *The logic of information*. Oxford: Oxford University Press.

Ford, N. (2015). *Models and theories in information behaviour research, chapter 7 in Introduction to information behaviour* (pp. 139–187). London: Facet.

Forster, M. (Ed.). (2017). *Information literacy in the workplace*. London: Facet.

Furner, J. (2010). Philosophy and information studies. *Annual Review of Information Science and Technology*, *44*, 161–200.

Furner, J. (2017). Philosophy of data: Why? *Education for Information*, *33*(1), 55–70.

Gorichanaz, T., Furner, J., Ma, L., Bawden, D., Robinson, L., Herold, K., ... Floridi, L. (2020). Information and design. Book symposium on Luciano Floridi's "The Logic of Information". *Journal of Documentation*, *76*(2), 586–616. https://doi.org/10.1108/JD-10-2019-0200/full/html

Jacobson, T. E., & Mackey, T. P. (2013). Proposing a metaliteracy model to redefine information literacy. *Communications in Information Literacy*, *7*(2), 84–91.

Koops, B., Newell, B. C., Timan, T., Škorvánek, C., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, *38*(2), 483–757.

Mackey, T. P., & Jacobson, T. E. (2014). *Metaliteracy*. London: Facet.

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192–199.

Mai, J.-E. (2019). Situating personal information: Privacy in the algorithmic age. In R. F. Jørgensen (Ed.), *Human rights in the age of platforms* (pp. 96–116). Cambridge, MA: MIT Press.

Makri, S., Blandford, A., & Cox, A. L. (2008). Investigating the information-seeking behaviour of academic lawyers: From Ellis's model to design. *Information Processing and Management*, *44*(2), 613–634.

Maletzke, G. (1963). *Psychologie der Massencommunikaton*. Hamburg: Verlag Hans Bredow Institut.

McMenemy, D. (2017). Privacy, surveillance and the information profession: Challenges, qualifications, and dilemmas?. University of Strathclyde. Retrieved from https://web.archive.org/web/20190815103808/https:/pureportal.strath.ac.uk/files-asset/70450065/cilip_privacy_briefing_mcmenemy.pdf.

McNicol, S., & Shields, E. (2014). Developing a new approach to information literacy learning design. *Journal of Information Literacy*, *8*(2), 23–35.

Meho, L. I., & Tibbo, H. R. (2003). Modeling the information-seeking behavior of social scientists: Ellis's study revisited. *Journal of the American Society for Information Science and Technology*, *54*(6), 570–587.

Mittelstadt, B. (2017). From individual to group privacy in big data analytics. *Philosophy and Technology*, *30*(4), 475–494.

Moore, A. D. (2010). *Privacy rights; moral and legal foundations*. Philadelphia: Pennsylvania University Press.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multidimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A—Mathematical, Physical and Engineering Sciences*, *374* (2083), 0118. https://doi.org/10.1098/rsta.2016.0118

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, the Journal of the American Academy of Arts & Sciences*, *140*(4), 32–48.

Pettigrew, K. E. (1999). Waiting for chiropody: Contextual results from an ethnographic study of the information behavior among attendees at community clinics. *Information Processing and Management*, *35*(6), 801–817.

Pinfield, S., Wakeling, S., Bawden, D., & Robinson, L. (2020). *Open access in theory and practice*. Abingdon: Routledge.

Poirier, E., & Robinson, L. (2014). Informational balance: Slow principles in the theory and practice of information behaviour. *Journal of Documentation*, *70*(4), 687–707.

Primiero, G. (2016). Designing systems with privacy: Formal and experimental methods. Retrieved from http://home.deib.polimi.it/schiaffo/TFI/lecture%202%20primiero.pdf.

Rawls, J. (1999). *A theory of justice*. Cambridge, MA: Harvard University Press.

Reynolds, P. D. (1971). *A primer in theory construction*. New York: Bobbs-Merrill.

Robertson, S. (2000). On theoretical argument in information retrieval, Salton Award Lecture SIGIR 2000. *SIGIR Forum*, *34* (1), 1–10. Retrieved from. http://sigir.org/files/forum/S2000/salton_lecture.pdf

Robinson, L., & Bawden, D. (2018a). Identifying good practices in information literacy education: Creating a multi-lingual, multicultural MOOC. In S. Kurbanoglu, J. Boustany, S. Spiranec, E. Grassian, D. Mizrachi, & L. Roy (Eds.), *Information Literacy in the Workplace. ECIL 2017. Communications in Computer and Information Science* (Vol. 810, pp. 715–727). Cham: Springer.

Robinson, L., & Bawden, D. (2018b). International good practice in information literacy education. *Knjižnica (Ljubljana)*, *62*(1), 169–185.

Robson, A., & Robinson, L. (2013). Building on models of information behaviour: Linking information seeking and communication. *Journal of Documentation*, *69*(2), 169–193.

Robson, A., & Robinson, L. (2015). The Information Seeking and Communication Model: A study of its practical application in healthcare. *Journal of Documentation*, *71*(5), 1043–1069.

Rønn, K. V., & Søe, S. (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, *34*(3), 362–378.

Rotman, D. (2009). Are you looking at me? Social media and privacy literacy. Poster presented at the iConference, Chapel Hill. Retrieved from https://www.ideals.illinois.edu/handle/2142/15339.]

Rubel, A., & Biava, R. (2014). A framework for analyzing and comparing privacy states. *Journal of the Association for Information Science and Technology*, *65*(12), 2422–2431.

Salton, G. (1980). A progress report on information privacy and data security. *Journal of the American Society for Information Science*, *31*(2), 75–83.

Savolainen, R. (2016). Conceptual growth in integrated models for information behaviour. *Journal of Documentation*, *72*(4), 648–673.

Savolainen, R. (2019). Modelling the interplay of information seeking and information sharing: A conceptual analysis. *Aslib Journal of Information Management*, *71*(4), 518–534.

Secker, J., & Coonan, E. (Eds.). (2013). *Rethinking information literacy: A practical framework for supporting learning*. London: Facet.

Solove, D. J. (2005). A taxonomy of privacy. *University of Pennsylvania law Review*, *154*(3), 477–564.

Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Stahl, B. C. (2008). Discourses on information ethics: The claim to universality. *Ethics and Information Technology*, *10*(2–3), 97–108.

Tavani, H. (2008b). Informational privacy: Concepts, theories and controversies. In K. E. Himma & H. T. Tavani (Eds.), *Handbook of information and computer ethics* (pp. 131–164). Haboken: John Wiley.

Tavani, H. T. (2008a). Floridi's ontological theory of information privacy: Some implications and challenges. *Ethics and Information Technology*, *10*(2–3), 155–166.

Tuominen, K., & Savolainen, R. (1997). A social constructionist to the study of information use as discursive action. In P. Vakkari, R. Savolainen, & B. Dervin (Eds.), *Information seeking in context* (pp. 81–96). London: Taylor Graham.

Van der Veer Martens, B. (2017). New grounds for ontic trust: Information objects and LIS. *Education for Information*, *33*(1), 37–54.

van Hoboken, J. (2019). The privacy disconnect. In R. F. Jørgensen (Ed.), *Human rights in the age of platforms* (pp. 255–284). Cambridge MA: MIT Press.

Vasalou, A., Joinson, A., & Houghton, D. (2015). Privacy as a fuzzy concept: A new conceptualization of privacy for practitioners. *Journal of the Association for Information Science and Technology*, *66*(5), 918–929.

Wacks, R. (2015). *Privacy: A very short introduction*. Oxford: Oxford University Press.

Walton, G. (2017). Developing a theory of information discernment. *Journal of Information Literacy*, *11*(1), 137–155.

Walton, P. (2014). A model for information. *Information*, *5*(3), 479–507.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Wilson, T. D. (1999). Models in information behaviour research. *Journal of Documentation*, *55*(3), 249–270.

Wilson, T. D. (2016). A general theory of human information behaviour. *Information Research*, *21*(4), paper isic1601. Retrieved from. http://www.informationr.net/ir/21-4/isic/isic1601.html

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy*, *11*(2), 378–389.

Woolf, V. (2002). Montaigne. In *The common reader*, (Annotated Edition) (pp. 58–68). Mariner: London and New York.

Wu, K., & Brenner, J. (2017). Philosophy of information: Revolution in philosophy. Towards an informational metaphilosophy of

science. *Philosophies*, *2*(4), 22. https://doi.org/10.3390/philosophies2040022

Wu, P. F. (2019). The privacy paradox in the context of online social networking: A self-identity perspective. *Journal of the Association for Information Science and Technology*, *70*(3), 207–217.

Wu, P. F., Vitak, J., & Zimmer, M. T. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, *71*(4), 485–490. https://doi.org/10.1002/asi.24232

**How to cite this article:** Bawden D, Robinson L. "The dearest of our possessions": Applying Floridi's information privacy concept in models of information behavior and information literacy. *J Assoc Inf Sci Technol*. 2020;71:1030–1043. https://doi.org/10.1002/asi.24367