Book Note

Privacy in Context: Technology, Policy, and the Integrity of Social Life
By Helen Nissenbaum
Stanford University Press (2010)
ISBN 978-0-8047-5237

Privacy in Context is a book in the theory of information privacy. It is written by Helen Nissenbaum, a well-respected expert and theorist in this field. While the book is theoretical in nature, the theory developed is meant to have direct practical application in evaluating new technologies and how they impact privacy. It therefore should be of interest to records and information practitioners and not just theorists.

The purpose of the book is to provide a framework that will guide ethical evaluation in the face of new information technologies and practices. Nissenbaum believes that the relevant fields of scholarship (e.g., law) and public debate are hampered by at least two problems: (1) existing ethical theories are too vague or abstract to help practitioners and the public. (2) the thinking of judges, lawyers, politicians, and the public at large is too much influenced by a distinction between what is private and what is public, i.e., the public/private distinction.

To remedy the flaws in the current theoretical landscape and provide a more practical approach, she works out in detail an account of privacy that she calls "contextual integrity." According to the theory of contextual integrity (CI), privacy consists in more than an individual's being able to exclude others from his/her personal information (access theory); and it is more than an individual's being able to control the flow of his/her personal information (control theory). Rather, privacy, in part, consists in an individual's personal information being accorded the appropriate treatment (flow) relative to a particular context and its associated information norms. In other words, even if a person's information has been accessed, acquired, and processed, the individual still has a legitimate claim to privacy and that claim concerns how the information is processed and disseminated. Further, proper processing and dissemination will be judged by what is appropriate for that information type within that particular context.

OVERVIEW OF THE THEORY

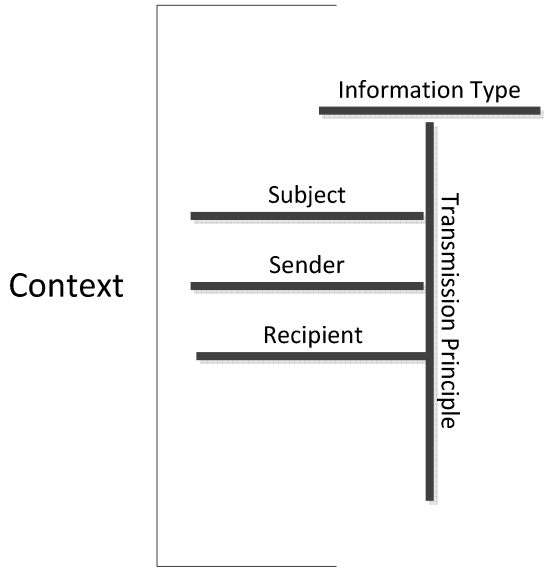
The core idea of the theory is that privacy issues arise when new technologies or practices threaten to change current information practices within a given context. The context consists of a set of parameters governed by information norms. To understand the factual circumstances of the potential threat to privacy and to evaluate it competently, it is necessary to understand the variables that make up the context and the information norms that govern it.

An information norm (or norms) applies in a context to what I will call an information structure.
A context is an institutional or social setting such as healthcare and friendship. Contexts are characterized by purposes (ends) and values, roles, activities, typical behaviors, expectations, etc. Some contexts, such as healthcare, are formal, with well-established protocols and explicit rules that serve well defined goals. Others, like friendship, are not formally defined, answering to a broader set of ends and accommodating more variegated activities and expectations. (Page 168)

An information structure has the following elements: (a) senders, (b) recipients, (c) data subjects, (d) information types, and (e) transmission principles. Information norms govern these structures. Senders are the persons or entities that cause information to be transmitted. Recipients are the individuals or entities that receive the information. Data subjects are the persons the information is about (and they can be the same as the senders). Information types are types of information, broadly construed (medical,

financial, biographical, etc.). Information types can be data elements such as identification numbers, names, and other attributes that would make up a database row. They can also consist of documents or sets of documents such as would make up a medical history or financial report. Transmission principles are the modes according to which the information is transmitted. Examples of transmission principles include reciprocity, symmetry, voluntary, confidential, etc., and their contraries, non-reciprocity, asymmetry, non-voluntary, and non-confidential. There are many such principles. These are just a few examples. An information norm governs and structures these elements. In some ways, it is made up of (constituted by) these elements. It is an expectation with a certain degree of social or moral force that the information type in question about the subject will be transmitted by the sender(s) to the recipient(s) according to the transmission principle.

The structure that information norms govern can be illustrated by the diagram below:



Crucial to contexts and information norms is the idea of a role. The actors (subject, sender, and recipient) are not just individuals or entities that can be named. They play or occupy social and institutional roles (e.g., friend, doctor, patient, religious guide, employer, insurer, etc.) This is no accident. Contexts are really made up of roles that are occupied by individuals and entities.

Examples of information situations structured by a context and its information norms can be found in an institution such as a hospital. In a hospital setting, the patient is the data subject, the recipients are the doctors or nurses, the senders are the doctors, nurses or patient; additional recipients can be other medical professionals, accounting/billing personnel, insurance companies and their employees, and others. Transmission principles that apply include asymmetry (between patient and medical attendants) and confidentiality. The end served by healthcare is the promotion of the individual's health and the promotion of public health. (See pages 171-174.)

While not explicitly stated in her account, the information structure she identifies can and should be iterated. As the example of the healthcare context suggests, the delivery of health services involves many activities, many actors, and many sub-goals. A real life application of Nissenbaum's CI model to health information flows would include multiple nodes with different actors and different transmission principles connecting each node.

THE DESCRIPTIVE AND NORMATIVE LEVELS

The theory of contextual integrity operates on two levels. The first level is descriptive; that is to say, it is a method for conducting a factual investigation and analysis of the privacy threatening technology or activity. The second level is normative. This means that it is a method for engaging in an ethical evaluation of the new technology or activity.

The descriptive application of the theory is relatively straightforward. Each of the parameters included in an information situation can be thought of as variable in relation to an existing information norm. When confronted with a technology or practice that appears to threaten privacy in some not yet articulated way, one can assess the nature and level of the possible changes by running through each variable. Has the sender (role) changed? In what way and to what degree? Have the recipients (roles) changed? Again, in what way? Are there more recipients? If so, how many more? Has their role changed? If so, how significantly? Has the data subject changed? If so, in what way? (For example, is the difference that the data subject is a minor?) Has the information type changed? For example, if the information was medical in nature, is the change that it now includes genetic data, when before it consisted in information about a virus or a type of symptom?) Finally, has a transmission principle changed? For example, was the information voluntarily obtained but now is captured without the subject's knowledge?

By applying the model to the new or proposed information situation, one can get a clearer, more detailed view of how the changes affect privacy. This makes it easier to evaluate them from an ethical perspective. In particular, it helps uncover profound changes that are often obscured by dogmatic distinctions such as that between what is public and what is private. For example, a proposal to digitize public records and make them searchable on the internet may not seem to be a significant departure from making the paper record available over the counter on the basis of a formal request. Nissenbaum's model can show that significant departures from the previous technologies and practices (paper, filing systems, request forms, etc.) follow from the proposal. The changes include a vast increase in the number of recipients as well as a change in transmission principles. The information consumer would not need to reveal his or her identity, would not need to expend much effort to obtain the information, and would be able to easily transmit it to someone else.

The normative component of the theory builds on the descriptive component. Once the descriptive work is done, one can evaluate the information system by considering the information norm in question and how it relates to its contexts. The investigation of the information situation will have included an investigation of the context in which it is situated and the information norms that have controlled this context. Because contexts (like healthcare, law enforcement, and commercial markets) have their own values (are built around and serve these values), the purposes or ends of theses contexts provide a basis for evaluating the changes caused by a new system or practice.

An example of how this work can be seen in the healthcare context. The end of healthcare, as mentioned above, is the promotion of individual and public health. If a new practice or technology is proposed, it needs to be evaluated by asking how it promotes the end of the context, in this case, promotion of individual and public health. So, if the technological practice proposed made it possible for medical professionals to warn individuals or the public that an individual had a contagious disease, this practice would have to be evaluated in light of the goal of healthcare. Depending upon the specifics of the case, arguments could be made on both sides as to the effect on the health of individuals and the public of such disclosures. An argument against disclosure would claim that individuals would be discouraged from seeking treatment if such disclosures were common. An argument for disclosure would claim that the progress of the disease could be stopped earlier. The important point here, however, is that the basis of the argument would be the goals of healthcare, as opposed to external considerations.

Nissenbaum's theory can be further clarified if we bring in an example of a practice that cannot be easily justified by appeal to the goals of the relevant context. Changing the example above just a bit, suppose

that the new technical practice proposed involved sharing personal medical data about diseases to pharmaceutical companies so that they could target marketing campaigns to only those persons with the disease. If the argument for this practice is that it would be commercially beneficial and economically rational, it would not have legs to stand on because these objectives are not central to the context of healthcare. The central goal of healthcare is promoting health. The only way for the advocates of this practice to get an argument off the ground is to link their commercial activity to the goals of healthcare. If a plausible case cannot be made that better marketing would promote the health of individuals and the public in general, the practice would not have justificatory legs to stand on.

The centrality of contexts and their defining values in the evaluation of new technology practices is the most novel part of the theory and can be of particular relevance for RIM practitioners. RIM professionals work within business and organizational contexts. They know these contexts and their institutions intimately and are therefore well positioned to apply the descriptive and normative components of the theory of contextual integrity to new technologies and practices. Further, as RIM practitioners, they are part of the context of the records and information management profession itself. Its goals and values will also be a source of guidance. For these reasons, it is clear that the ideas at the heart book resonate well with RIM practice and should be studied and applied to the contexts in which RIM professionals work.

RIM professionals will find useful a decision procedure sketched out on page 172 and summarized below:

1. Describe the information flows of the technology/practice.
2. Identify the context.
3. Identify the information situation (subjects, senders, recipients, and transmission principles).
4. Identify the information norms.
5. Assess the nature and degree of change.
6. Evaluate the situation in terms of standard moral principles.
7. Evaluate the situation in terms of the ends/purposes/values of the context.
   (Page 182)

CRITICAL COMMENTS

It should be noted that the theory is meant to be a corrective to the traditional method of analysis which takes high level moral rules and applies them to new technologies and practices. These principles, e.g., the principle of fairness, the principle of autonomy, or the principle of non-harm, are very general. Nissenbaum rightly argues that they cannot be easily applied to new technologies because of their generality. By contrast, the purposes and ends of the contexts themselves fit the factual circumstances closely because the contexts are built around them. These context relative purposes, therefore, should be the normative engine of ethical evaluation for new technology practices.

Because it is so important to the polemic of the book to elevate the role of contextual ends and values, her exposition tends to obscure, rather than clarify the relation of high level moral principles to more specific and contextually relevant moral rules. This may be because Nissenbaum's normative theory is very much animated by the work of a political philosopher, Michael Waltzer, who sees justice as a multifaceted concept that separates into different spheres that operate according to their own principles. (See *Spheres of Justice*, 1986) As a result, she tends to treat steps 6 and 7 as if they were independent and as if step 6 serves as little more than a basic check to see if any fundamental moral rules or basic rights are available to settle the issue. They usually are not, as they are either too vague or cancel each other out. So, having ruled out from the analysis anything obvious, one can move on to step 7 and see what the context relative ends have to tell us.

The problem is that this presents a very compartmentalized approach to ethical analysis that is not likely to be as effective as it could be. Consequently, her analyses of a number of cases are quite weak. Below are two examples:

Commercial Markets: On page 209, Nissenbaum considers the practice of price discrimination based on the capture, aggregation and mining of personal data. By better understanding customers purchasing behaviors (based on personal data profiles), they can be sorted into categories and offered different prices for the same products. Nissenbaum's initial objections are based on the moral principles of step 6. These objections are her strongest. Latter (page 213), she attempts an argument based on the contextual values (step 7). But the arguments are unconvincing. The values and ends of commercial markets are the creation of wealth and the rational allocation of resources. Price discrimination may advance these goals well, even if a strong moral argument can be made against the practice. The problem for Nissenbaum's model is that the practices that make up social contexts need to be evaluated from the perspective of our common morality and their ends and goals must be integrated into a just and moral society. Step 7 cannot carry its own weight outside of the framework of our common morality.

Law Enforcement: The same issue arises for the context of law enforcement. On pages 215-216, Nissenbaum briefly discusses the issue of national security, terrorism and law enforcement and brings up the issue of wiretapping. This is an area where contexts should and have been considered in law, policy and ethics. More fine grained rules could be developed by paying attention to the details of the information situation (the descriptive element of the theory). But the end of law enforcement is to protect individuals from criminal activity. More often than not, the capture and processing of personal information advances that goal. The problem is that the ends and activities of law enforcement are constrained in the United States by other political and moral values. Unless Nissenbaum wants to treat the entire society as a social context (which she seems to do on page 216 and which would completely enervate the concept of a context), her theory and decision model does not look particularly powerful in the case of law enforcement (though there may be exceptions.)

Despite this last criticism, I think the book provides a useful framework for working through policy questions in light of new technologies and practices. The method of analysis summarized in Nissenbaum's decision model can be improved by simply recognizing that steps 6 and 7 should not treated as independent analyses answering to different value dimensions. Rather, they should be seen as integrated, with the context relative norms and ends falling within the framework of broader moral values. Moral knowledge falls on a continuum with abstract principles on one end and particular judgments on the other. In between are a multitude of rules, some more general (e.g., do not deceive) and some more specific (do not disclose sensitive personal data to third parties). Nissenbaum's context relative values and ends provide a basis for working out more specific rules but they do not form the only basis. Further, whatever rationale or moral grounds they do provide has to be integrated into the larger system of moral principles. They cannot stand on their own.

Properly integrated, the theory of contextual integrity provides an excellent framework for analyzing information privacy issues. Readers will also benefit from the ample cases discussed and the focus on the disruptive aspect of information technology. RIM professionals will certainly be able to apply its key concepts to their work. They will also find that these ideas implicitly validate the role the RIM practitioners can and should play in their organizations and society at large in creating ethical information practices and policies.

Norman Mooradian, Ph.D.
www.ethicalcomputing.net
norman.mooradian@ethicalcomputing.net