Information Polity 16 (2011) 391–395
DOI 10.3233/IP-2011-0257
IOS Press

Book Review

Waiting for the barbarians or shaping new societies? A review of Helen Nissenbaum's *Privacy In Context* (Stanford: Stanford University Press, 2010)

Helen Nissenbaum's *Privacy In Context* [3] is set to become a seminal work, both for privacy scholars around the world and for many other researchers who increasingly deal with privacy-related topics. Indeed, this is a much-awaited book, advancing the theory of privacy as 'Contextual Integrity' presented in an often-quoted article back in 2004 (cf. [2]). Moreover, the idea of Contextual Integrity proves generally very seductive for its claim to offer a break from academic debates that have reached a 'dead-end' and its ambition to return to everyday problems of an 'information age society', promising a way-out or at least a decisional matrix. All these elements, and many more that will be discussed below, justify the acclaimed status of Nissenbaum's work.

Nevertheless, when reading the book from a different point of view, both in terms of research interests and disciplinary posture, some elements of the 'Contextual Integrity theory' become less innovative and more debatable. For this reason, this review tries to presents a synthetic but fair description of the theoretical framework developed by Nissenbaum, pinpointing the most interesting choices and insights. Then, it advances three remarks to the attention of researchers dealing with privacy (and data protection) in Europe; and, finally, it attempts to raise a more substantial critical objection to the framework itself.

First of all, it should be said that during the six years that have elapsed between the 2004 article and the 2010 book, 'privacy' has had a stable place towards the top of public and academic debates, remaining a recurrent hot topic in the news and in policy-making. Notwithstanding such emphases and interest on the topic, conceptualising privacy remains a highly challenging and contested activity. As Nissenbaum reminds us, one of the few points of agreement among privacy scholars is that "privacy is a messy and complex subject" [3, p. 67].

Indeed, one of the most positive feature of the book is Nissenbaum's capacity to develop a structure both extremely useful to build her argument as well as to help the reader to step into complex debates and issues. The structure revolves around the questioning of the ability of privacy theories to describe, explain and assess privacy claims raised by the introduction of new socio-technical systems. The book is composed of three main parts: the first introduces and describes the main socio-technical systems that could threaten privacy; the second presents the most relevant theories of privacy developed by (mainly US) scholars and the key issues and debates among them; and, finally, the third part advances an enhanced conceptualisation of the theory of Contextual Integrity. Both the second and the third part devote attention to the possible 'implementation' of theories, including Contextual Integrity.

The decision to devote the first three chapters (comprising Part I) to a taxonomy of the main trends in terms of socio-technical systems dealing with personal information is surely coherent with the aim of the book, but it is also an idea to be strongly welcomed for several reasons. Firstly, the decision to start with actual and emerging practices creates a point of entry into the topic for an audience beyond privacy-focused academics, advocates or experts. Furthermore, the taxonomy proposed by Nissenbaum is at the same time very comprehensive and very clear, providing the necessary elements to grasp issues that frequently appear obscure. She divides practices into three main categories: monitoring and tracking (ch. 1); aggregation and analysis (ch. 2); publication and dissemination (ch. 3). Finally, her very choice of

working with the concept of 'socio-technical systems' is particularly interesting. She is probably among the few privacy scholars who try to take stock of the important literature, and scientific insights, of the rich and protean field of Science, Technology and Society. All these features are important assets of the book, providing a useful tool (and cartography) for researchers from a variety of different disciplines.

The second part of the book also introduces a sort of double taxonomy. In chapter four, Nissenbaum presents in a concise but exhaustive manner the main theories of privacy developed in the United States. The goal is ambitious, but the author succeeds in mapping scholars and ideas around three main divides: (i) normative vs. descriptive accounts; (ii) privacy as 'access' vs. privacy as 'control' emphasis; (iii) privacy as protection of a specific realms vs. privacy as protection of other important values. This chapter is a valuable asset for researchers, because it integrates a wide range of complex literatures and provides the basic tools to further understand the issues at stake and the rationale of Nissenbaum's argument.

The remainder of Part II presents the important US debate over the private/public dichotomy, concerning the 'scopes' of privacy and whether privacy claims should be confined to intrusions to the private sphere or can also be raised in relation to public activities. These two chapters serve the double aim of presenting one of the main discussions surrounding privacy in the US, and, at the same time, establishing some of the premises for the development of a new theory of privacy, able to bypass the deadlocks and incoherencies of the most established theories. Indeed, the position of the author is that "[a]pproaches to privacy that restrict its sphere of legitimacy to the private (. . .) are founded on a set of assumptions about the relationship between privacy and the public/private dichotomy that ultimately are incoherent" [3, pp. 125–126]. Not only particularly relevant for the 'economy' of Nissenbaum's theory, these two chapters will also attract the attention of US privacy scholars and many surveillance studies researchers.

Finally, the third part of the book is the core of the publication. After having highlighted the shortcomings of other privacy theories, Nissenbaum advances a comprehensive conceptualisation of her own theory. In her own words, the shift proposed is to understand privacy "neither [as] a right to secrecy nor [as] a right to control but [as] a right to *appropriate* flow of personal information" [3, p. 127].

To fully understand what Contextual Integrity is, it is important to introduce both the underpinning assumption, some specific terminology, and its descriptive and normative aim. The main assumption is that "we act and transact not simply as individuals in an undifferentiated social world, but as individuals acting and transacting in certain capacities as we move through, in and out of a plurality of distinct social contexts" [3, pp. 129–130]. Contexts are "structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)" [3, p. 132]. Several specific "constructs" are relevant to the conceptualization of Contextual Integrity, however, the most relevant is the one of "context-relative informational norms" which "prescribe, for a given context, the types of information, the parties who are the subjects of the information as well as those who are sending and receiving it, and the principles under which this information is transmitted" [3, pp. 140–141]. It is also important to highlight the fact that "context-relative informational norms" subsume a "co-constitutive relationship between informational norms and contexts" [3, p. 141].

The aim of the theory of privacy as Contextual Integrity is to provide a decision heuristic to apply when new socio-technical systems intervene in a context. Then, the Contextual Integrity framework would apply in three key moves: (i) explanation; (ii) evaluation; (iii) prescription. In the first move, Contextual Integrity "functions as a metric that is sensitive to meaningful changes affecting people's reactions to new systems or practices" [3, p. 190]. With the second move, the decision heuristic evaluates the possible violation of context-relative informational norms, "comparing altered flows in relation to those that were previously entrenched" and it judges eventual conflicts between the "moral and political values"

of new socio-technical systems and those of the context(s) at stake [3, pp. 190–191]. Finally, the third move relies on such evaluation to decide over the introduction of the new socio-technical systems. An operational version of the framework is also named "augmented contextual integrity decision heuristic" and introduces a detailed, step-by-step, ready-to-use script of action [3, pp. 181–183].

In the last chapter, Nissenbaum sketches some applications of the framework of Contextual Integrity to case studies representative of the three trends developed in the first part of the book. This 'implementation' exercise is developed further in the conclusions, where she compares the application of Contextual Integrity to the US doctrine of 'reasonable expectation of privacy'.[1] In particular, she proposes to strengthen the 'reasonable expectation of privacy' test operated by US judges with key elements of the Contextual Integrity framework. This would reduce the arbitrariness side of the test, because it would suggest to judges and other decision makers "where they should be looking for relevant norms, which similar cases constitute reasonable analogies and which do not" [3, p. 235].

Compared to the 2004 article, the book does not bring substantial changes to Nissenbaum's theoretical and normative framework. However, the book serves to fortify her argument in a number of areas, and these areas are mostly well chosen. In particular, the book provides for an enriched set of case studies and socio-technical systems; it offers a more developed presentation of the social science roots of the theory, in particular fields' theories and Michael Walzer's strong influence; it replies in more extensive ways to some of the possible 'worries' linked to Contextual Integrity; and, finally, it further clarifies the link with the US doctrine of 'reasonable expectation of privacy'.

All these elements contribute to the construction of what appears to be a sound and solid theory of privacy, a theoretical and normative framework particularly appealing for the growing wave of studies on surveillance and for the proponents of the adoption of privacy impact assessments. Nevertheless, despite the coherence of the work, some remarks and critiques could still be advanced.

The following three remarks are rather Eurocentric and mainly addressed to the attention of Europe-related researchers. The first concerns the 'asymmetrical' relevance of Nissenbaum's discussion on the private/public debate. This debate is still an important one in the US where the 'reasonable expectation of privacy' does not seem to offer a solid and foreseeable tool to protect privacy in public. But in Europe, the claim for the protection of privacy in public has been already supported by the case law of the European Court of Human Rights (ECtHR). Indeed, the ECtHR has granted a 'sensible extension' of the application of the article 8 of the European Convention of Human Rights (ECHR), now covering also public private information on the base of the nature of their processing (including a case involving the use of CCTV in public, Peck v. United Kingdom 2003), or to support the establishment of social relations in public and working spaces (Niemetz v. Germany 1992) [5, pp. 410–414].[2]

The second remark concerns the shrinking of privacy and data protection into a single 'element' within the vision of Contextual Integrity. This posture is partially at odds with current developments in the legal framework of the European Union (EU), where the EU Charter of Fundamental Rights fosters a process of quasi-constitutionalisation of privacy and data protection as two different rights. While it is true that the relationship between the two is still an open issue (cf. in extenso [1]), the 'potential' of two different rights would probably request a more explicit bridging between them and Contextual Integrity.[3]

[1] The so-called 'reasonable expectation of privacy' test finds its roots in the famous case Katz v. United States, in 1967. In his concurring opinion, Justice Harlan advanced a two-fold requirement to identify the relevant scope of privacy: "[first] a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'" (quoted in [4, p. 226].

[2] The author thanks Gloria González Fuster for pinpointing and discussing this issue with him.

[3] For example, while it is true that the 'classical' Fair Information Principles are mirrored in both US and EU relevant legislations, they have been further refined and developed somehow in different ways.

Finally, the test introduced by Nissenbaum's decision heuristic is not only similar to the US doctrine of 'reasonable expectation of privacy', but it also mirrors some of the steps of the ECtHR test (Is there any interference? Is this interference justified according to the specific criteria/respect of values?).[4] This ECtHR test, and in particular the second step concerning the criteria of legality, proportionality and necessity in democratic societies, is increasingly and explicitly adopted outside the scope of the ECHR, for example by the European Commission and other EU institutions, *inter alia* in the assessment of new security measures. Most probably, any European-related application of the theory of Contextual Integrity would benefit from a comparative analysis of the two frameworks.

As noted above, these remarks are mainly a call for researchers working on European-related topics to evaluate what could be 'local' theoretical and legal practices before adopting *tout-court* a Contextual Integrity framework. In fact, Helen Nissenbaum acknowledges in the introduction the limitation of her work in terms of the scope of her 'sources'. However, the strong transnational nature of socio-technical systems and the on-going transatlantic negotiations touching on privacy (and data protection) would have merited an explicit discussion of the potential and limits of Contextual Integrity outside the US theoretical and legal practices.

Now, moving from the previous remarks to a more substantial critique of *Privacy in Context* is particularly challenging. Its internal structure and the coherence among assumptions, ambitions and conclusions tend to pre-empt any real critique of the theory, especially when seen from outside her discipline. Nonetheless, a point of entry could be to follow the very idea of Contextual Integrity as a theoretical shift from conceptions of privacy as 'control' and/or 'access', and thus decrypt the other shifts engendered by this move. A first, quite explicit, shift is from the protection of individuals and their relations to the protection of relatively institutionalised contexts (an important element of the evaluation process of the Contextual Integrity heuristic is to identify the relevant context, which presupposes a certain degree of established recognition of the same). Within these contexts, it seems to rule a sort of continuous consensus, threatened only by external socio-technical systems. One of the explicit aims of Nissenbaum is to sift legitimate claims to privacy from non-legitimate ones. However, in this sense, the descriptive value of the theory seems to fully leave the ground to the normative goal of achieving the highest degree of Contextual Integrity according to a previous 'privacy-issues-free' *status quo*.

This is not a merely conservative posture, but one that tries to evacuate the mapping of the actual political uses of privacy (and data protection), if not to evacuate most of politics. Think about the use of privacy or data protection for contesting the integrity of an established context from within, for example when personal data are already processed by an existing socio-technical system deemed to by legitimate by the lack of public debate or even by the consensus of the majority. Or, on a quite opposite note, think about the discursive rhetoric of many EU-US agreements claiming to protect and enforce data protection, but *de facto* establishing new security systems.

Probably Contextual Integrity would discard many of these privacy claims as not legitimate, thus sidelining the politics of privacy to favor a mostly pre-settled moral balancing. Here, a second shift occurs, one that relegates privacy in a sort of 'political vacuum', where 'contexts' appear politics-free, empty of constitutive struggles or power relations. In a sense, privacy as Contextual Integrity is no more

[4]The test is based on the wording of article 8 of the Convention: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

a potentially constructive force, especially in relation to contexts, but it merely limits itself to preserve them.

Where are the actors? Only contexts, and related values and rules, seem to count. Even in the socio-technical systems, again contexts are the only 'social' agent, with the paradoxical effect that the only possible variable that is really taken seriously into consideration relates to the agency of technology, even if considered in relatively flexible ways. Subjectivities emerge rarely, popping-up only when the framework of Contextual Integrity requires spelling out recipients, senders and (data) subjects. But privacy seems far from them, protecting values and ends instead of being a tool in the hand of actors, waiting for the barbarians at the external borders instead of shaping new societies.

Rocco bellanova

CReSPo- Facultés universitaires Saint Louis & LSTS- Vrije Universiteit Brussel.

References

[1] Gutwirth, Serge, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt, eds, Reinventing Data Protection? Dordrecht: Springer, 2009.
[2] H. Nissenbaum, Privacy as Contextual Integrity, *Washington Law Review* **79** (2004), 119–158.
[3] H. Nissenbaum, *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010.
[4] D.J. Solove, M. Rotenberg and P.M. Schwartz, *Information Privacy Law*. 2nd ed., New York: Aspen, 2006.
[5] F. Sudre, *Droit Européen Et International Des Droits De L'homme*, 7ème édition refondue ed., Paris: Presses Universitaires de France, 2005.