"RESPECT FOR CONTEXT": FULFILLING THE PROMISE OF THE WHITE HOUSE REPORT[1]

Helen Nissenbaum

In February 2012, the Obama White House unveiled the Consumer Privacy Bill of Rights (2012, 9) embedded in a comprehensive report, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." The report and bill of rights, which signaled direct White House interest in privacy and buoyed hopes that change might be in the air, were cautiously endorsed by a range of parties—public interest advocates, industry leaders and associations, and government agencies—who have disagreed with one another on virtually everything else to do with privacy.[2]

Of the seven principles proposed in the Consumer Privacy Bill of Rights, six are recognizable as kin of traditional fair information practices, embodied, for example, in the OECD Privacy Guidelines. The third principle of "Respect for Context" (PRC), the expectation that "companies will collect, use, and

Helen Nissenbaum is professor of media, culture and communication, and Computer Science, at New York University, where she is also Director of the Information Law Institute.

disclose personal data in ways that are consistent with the context in which consumers provide the data" (p. 47), is intriguingly novel. *Context*, however, is a mercilessly ambiguous term with potential to be all things to all people. Its meanings range from the colloquial and general to the theorized and specific and shades in between. If determining the meaning of *context* were not challenging enough, determining what it means to respect it opens further avenues of ambiguity.

From a virtually endless set of possibilities, four interpretations are particularly interesting: context as technology platform or system, context as business model or practice, context as industry or sector, and context as social domain. Which one is the right one is the question I address in this essay. As I argue below, whether the Privacy Bill of Rights fulfills its promise as a watershed for privacy, whether the principle of respect for context is an active ingredient in the momentum will depend on which one of these interpretations drives public and private regulation going forward.

Although other interpretations have appeared in connection with privacy, I focus on these four because they imply divergent policy directions and also because they reflect persistent voices in discussions leading up to and following the White House report.

Context as Technology: In more than one hundred years of worrying about privacy, technological development has been a major impetus for societal attention. The contemporary moment is a case in point with a focus on the realm of information and digital networks—the Internet, and the myriad platforms and systems sitting atop (or below) it, such as mobile devices, e-mail, social networks, cloud service, and the Web itself. Most

of us readily talk of communication and transaction taking place *online* or *in* cyberspace and see associated privacy problems as distinctive to these electronically mediated contexts. It is a short distance to conceive of this technological substrate and its social networks, Twitter, Wikipedia, mobile apps, and location-based services as a context. In such instances material properties of respective media, systems, or platforms shape—moderate, magnify, enable—the activities, transactions, and interactions that they mediate, as well as the ways information is tracked, gathered, analyzed, and disseminated. *Respect* for contexts, under this interpretation, would require policies to be heedful of systems' and platforms' natural function.

Context as Business Model or Practice: According to this interpretation, it is not technology per se that defines privacy rules of the road but distinctive business models and practices. Interpreted as the model or practice of a particular business, context is shaped by the nature and aims of that business and the practices it pursues in order to achieve these aims. This is an interpretation supported in the comments of many incumbents in the IT and information industries. Taking Web search as an example, whereas the underlying technological system may accumulate search logs containing information about personally identifiable individuals, the business model may define how long the logs are kept, how they are used, and with whom they are shared.

Context as Industry or Sector: Adopting the interpretation of context as sector or industry broadens the unit of analysis from individual businesses to the sector of industry in which they function. It also is compatible with the prevailing sectoral policy environment in the United States, which largely has

regulated privacy protection on a sector-by-sector basis. By merging sector and industry I am not suggesting their meanings are identical but acknowledging that those who favor this interpretation have used these terms interchangeably in their comments. According to this interpretation, respect for context would amount to adherence to the set of rules or norms developed by, for, and within respective sectors or industries.

Context as Social Domain: This interpretation, supported by the theory of contextual integrity, presents contexts as social spheres, constituents of the differentiated social space of everyday life, including instances such as education, health care, politics, commerce, religion, family and home life, recreation, marketplace, and work. Spheres generally comprise characteristic activities and practices, functions (or roles), aims, purposes, institutional structure, values, and action-governing norms. Norms governing the flow of information form a subclass of these norms; context-specific informational norms (from here on, "informational norms") are crucial to contextual integrity. To flesh out what it would mean to respect context as social sphere requires a brief detour through the theory of contextual integrity.

Where other accounts of privacy focus on exposure of personal information or loss of control by data subjects, the theory of contextual integrity cites appropriateness of flow, namely those data flows that comport with legitimate informational norms, as a fundamental tenet. Whether a particular flow, or transmission of information from one party to another, is appropriate depends on the type of information in question, about whom it is, by whom and to whom it is transmitted, and the conditions or constraints under which this transmission takes

place. According to contextual integrity's model of information flow the critical parameters are identified as: *Actors*—subject, sender, recipient—ranging over context-relevant functions, or roles, or acting in capacities associated with respective contexts. These functional roles include the familiar—physician, nurse, patient, teacher, senator, voter, polling station volunteer, mother, friend, uncle, priest, merchant, customer, congregant, policeman, judge, and, of course, many more. The parameter of *information type*, likewise, ranges over variables derived from the ontologies of specific domains. In health care, these could include symptomologies, medical diagnoses, diseases, pharmacological drugs; in education, they may include cognitive aptitude, performance measures, learning outcomes; in politics, party affiliations, votes cast, donations; and so forth. *Transmission principle*, the third parameter, designates the terms, or constraints, under which information flows. Think of it as a sluice gate. Abstractly conceived, the transmission principle has not been explicated in scholarly or policy discussions even though, in practice, its role in social convention, regulation, and law is pivotal. Control over information by the information subject can, in its terms, be understood as but one (albeit an important one) among an extensive range of options, including "in confidence," "with third-party authorization," "as required by law," "bought," "sold," "reciprocal," and "authenticated."

It bears emphasizing that the three parameters—actors, information type, and transmission principles—are independent. None can be reduced to the other two, nor can any one of them carry the full burden of defining privacy expectations. This is why past efforts to reduce privacy to a particular class of information (say, "sensitive" information) or to one transmission

principle (say, control over information) were doomed to fail. For decades, these reductive efforts, in my view, have invited ambiguity and confusion in our understanding of privacy and have hindered progress in attempts to regulate its protection. Control over information may be an important transmission principle, but always with respect to particular actors and particular information types, all specified against the backdrop of a particular social context.[3]

Contextual integrity is achieved when actions and practices comport with informational norms. It is violated when actions or practices defy expectations by disrupting entrenched or normative information flows. Because informational norms model privacy expectations, it is no surprise when people react with annoyance, indignation, and protest when contextual integrity has been violated. Contextual integrity thus offers a diagnostic tool with prima facie explanatory and predictive capacities, providing a more highly calibrated view of factors relevant to privacy than traditional dichotomies such as disclose/not disclose, private/public.

Diagnosing a disruption in entrenched flow is but a start; being able to *evaluate* it is crucial to the moral sway of contextual integrity. Disruptive technologies, such as enhanced health indicators; new forms of communication and association, such as through social networks; and information search tools online offer great value. How to distinguish positive opportunities from those that violate privacy is an important challenge. To meet it, contextual integrity calls for a comparative assessment of preexisting flow against novel flow involving three layers of analysis: One considers the interests of key affected parties—the benefits they enjoy, the costs and risks they suffer. This largely

economic approach, which dominates the policy arena in standard stakeholder analyses, offers only a partial view of what is at stake. A second layer considers general moral and political values. Thus, beyond straightforward trade-offs that might optimize overall benefit, this layer enjoins us to consider whether costs and benefits are justly distributed. Other core values identified in the privacy literature are democracy, unfair discrimination, informational harm, equal treatment, autonomy, identity formation, and a range of civil liberties.[4] Finally, we must consider context-specific values, ends, and purposes. These may help resolve conflicts that have long stumped us, such as privacy versus security, privacy versus profit, and so forth. A contextual analysis may reveal that freedom should trump in a given context, say a library, while security in another, say an airport. Contextual integrity offers a thoughtful way beyond the banal dichotomies of privacy versus business interests, versus national security, public safety, and freedom of expression. This layer insists that privacy, as appropriate information flows, serves not merely the interests of individual information subjects, but also contextual, social ends and values.

According to this account of context as social domain, *respect for context* is respect for contextual integrity.

To see why this account is the only one of the four with the potential to bring about significant advancement in protecting privacy, we take a closer look at the White House Privacy Bill of Rights. The debt to traditional "Fair Information Practices" (FIPs) is clear with principles of transparency, security, access and accuracy, and accountability, which line up with equivalent FIPs; respect for context, however, is not linked with any

single principle but associated jointly with two equivalents: purpose specification ("The purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with these purposes and as are specified on each occasion of change of purpose" [p. 58]) and use limitation ("Personal data should not be disclosed, made available or otherwise used for purposes other than those specified . . . except . . . (a) with the consent of the data subject; or (b) by the authority of law" [p. 58]).

But purposes are not given in the principles themselves, resulting in a code that is either admirably adaptable or substantively empty. Purpose specification is the wild card, potentially creating a Trojan horse out of use limitation, collection limitation (often called data minimization), and even security and data quality. Unless and until purposes are shaped by substantive requirements, FIPs constitute a mere shell, formally defining relationships among the principles and laying out procedural steps to guide information flows.[5]

Whether the Consumer Privacy Bill of Rights devolves to this procedural formulation of FIPs or fulfills its promise of positive change depends on how we interpret context. I have argued that context understood as social domain is the most viable basis for progress among the four alternatives we have considered.

Under the interpretation of context as business model or practice, context would be determined by the exigencies of a particular business and ensuing policies, presumably communicated via terms of service. For online commerce, a merchant may reasonably require a consumer's address and valid

payment information, but if business purpose is a blank check and political economy is all that shapes the relationship between the information collector and information subject, there is no recourse to standards beyond business expedience. By definition, each business entity determines what is and is not expedient. This may mean buying and selling information resources, extracting information resources from transactions, and using information with no restriction (except in the few sectors covered by privacy legislation). Even admitting the importance of business to society, its parochial needs are not sound footing for privacy's moral imperative.

What about context as technology platform or system? It is quite sensible to refer to a Facebook profile, a Bing search, a Fitbit group, the Web, and an e-mail exchange as contexts, but a mistake if respect for context is a bellwether for privacy. Letting technological affordance define moral imperative would mean that platform or system not only determines what information flows *can* happen but what flows *ought* to happen. Doubtless technologies shape contexts, may even constitute them. They alter practice and sometimes pull norms and standards along with them. New technologies may reconfigure ontologies, yield new categories of information, new types of actors and modes of dissemination. These may rightly call for a review of entrenched norms and spur new norms where none previously existed. But allowing these systems fully to account for the meaning of respect for context allows material design to define ethical and political precepts. It leads to distortions in regulation, responsive to details of technology outside its social significance. This places these systems beyond the pale of normative judgment, but where respect for context is a bellwether for privacy, it is a

mistake to confuse technological contexts with those that define legitimate privacy expectations.

Interpreting context as sector or industry, which aligns well with the U.S. sectoral approach to privacy regulation, overcomes some of the drawbacks of context as business model because, instead of devolving to policies serving the interests of individual businesses, norms of information flow would be guided by a collective mission—ideally, collective best practice. Including sectors beyond industry and business, such as education, health care, politics, family, or religion, could extend the range of *appropriate* informational rules beyond serving parochial interests of business incumbents. Yet, ironically, as the scope of sectors is broadened, their conception edges in the direction of social spheres around which the theory of contextual integrity is oriented.

Interpreted as respect for contextual integrity, the principle of respect for context would require information flows to be characterized in terms of information types, actors, and transmission principles and evaluated in terms of the balance of interests and impacts on values and contextual aims. Such evaluations extend beyond conventional stakeholder interests and even beyond the general moral and political values widely acknowledged in privacy discussions. Context is not only a passive backdrop against which the interests of affected parties are measured, balanced, and traded off. In addition, context defines *how* these interests and values should be weighed. The integrity of contexts *themselves* is a final arbiter of information practices—vibrant marketplace, effective health care, sound education, truly democratic governance, and strong, trusting families and friendships.

In sum, for the Consumer Privacy Bill of Rights to advance privacy protection beyond its present state, much hangs on how context, in the principle of respect for context, is understood. Four contenders jockey for preeminence: business model, technology, sector, and social domain. I have argued that the fourth holds the greatest potential. Respecting context as *business model* offers no prospect of advancement beyond the present state of affairs. Respecting context as *sector* (or industry) fares somewhat better, though how much better this approach meaningfully advances privacy protection depends on how sectors are defined. The problem is particularly acute for the "information sector," where the proverbial fox would be guarding the henhouse. Further, if industrial sectors dominate the way sectors are conceived, the influence of sectors such as health care, education, religion, and politics will be diminished, or the commercial aspects of these industries may play a disproportionate role. A purely technological understanding of context would mean technical affordances and constraints would define legitimate expectations of privacy. But so doing gets things exactly backward, draining respect for context of moral clout. Our morally legitimate expectations, shaped by context and other factors, should drive design and define the responsibilities of developers, not the other way around.

According to the interpretation of context as *social domain*, respecting context means respecting informational norms that promote general ethical and political values, as well as context-specific ends, purposes, and values. Informational norms must specify all relevant parameters—actors (functioning in roles), information types, and transmission principles—or yield rules that are partial and ambiguous. In revealing critical

dependencies between social values and appropriate information flows, contextual integrity once and for all debunks the fallacy of privacy as valuable for individuals alone.

Contexts are shaped by technology, business practice, and industry sector. They may also be constituted by geographic location, relationship, agreement, culture, religion, and era, and much more. In individual cases, any of these factors could qualify and shape peoples' expectations of how information about us is gathered, used, and disseminated. No one of them, however, provides the right level of analysis or carries the same moral and political weight as social domain. Accordingly, I offer an amendment to the Consumer Privacy Bill of Rights's principle of respect for context:

Respect for context means consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the [social] context in which consumers provide the data.

NOTES

1. This essay is drawn from a longer article greatly indebted to Solon Barocas, Emily Goldsher-Diamond, Mike Hinze, Chris Hoofnagle, and James Rule. The project was supported by NSF CNS-1355398 and DGE-0966187 and the Intel Science and Technology Center for Social Computing.

2. See M. Hoffman, "Obama Administration Unveils Promising Consumer Privacy Plan, but the Devil Will Be in the Details," Electronic Frontier Foundation, 2012; D. Hoffman, "White House Releases

Framework for Protecting Privacy in a Networked World," *Policy@ Intel* blog, February 23, 2012; "White House Unveils Consumer Privacy Bill of Rights," *EPIC Alert,* 19.04, February 29, 2012; and C. Civil, "President Obama's Privacy Bill of Rights: Encouraging a Collaborative Process for Digital Privacy Reform," *Berkeley Technology Law Journal,* March 12, 2012.

3. See H. Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford, CA: Stanford Law, 2010) for a full account.
4. See Nissenbaum, *Privacy in Context,* especially part 2.
5. Ibid.

PRIVACY, AUTONOMY, AND INTERNET PLATFORMS

Frank Pasquale

When do Internet platforms start stunting users, rather than enabling them to become what they want to be? Facebook's recent psychology experiment sharply poses that question for those on both sides of the platform.[1] Ordinary Facebookers, resigned to endure ever more intrusive marketing manipulation, were thrown for a loop by the news that they may be manipulated for no commercial reason at all. Researchers inside Facebook (and their university collaborators) saw their own identity questioned. Were they true scientists or some new kind of inquirer?

It's time to deepen the story of the experiment as a "loss of autonomy," by connecting the strictures imposed on insiders and outsiders. Ordinary users can't access, challenge, or try to adapt the code that Facebook uses to order their news feeds, except in the crude and stylized ways offered by the company. Social scientists have to play by Facebook's rules to get access to the data they need—and we can probably assume that a more informed consent process was either tacitly or explicitly rejected as too much of an interference with the ordinary business of

Frank Pasquale has taught information and health law at Seton Hall since 2004.