Helen Nissenbaum

Privacy in Context

In the past few decades, a radical intensification in socio-technical practices of capturing, storing, manipulating, and disseminating information about people (henceforth, "personal information") has aroused suspicion, indignation, and vocal protest not only among legal experts, social critics, and privacy advocates, but also in the popular media and the general public. Public debate and disputation have accompanied the introduction of such systems as Caller ID, Lotus Marketplace Households, EZ Pass, Carnivore and "total information awareness", online profiling, Choicepoint, Radio Frequency Identification, biometrics, CCTV, and one that has recently engrossed me, wholesale logging of Web-search queries. Everywhere we turn, in every transaction we engage, in all our behaviors, someone seems ready to capture, store, analyze, and distribute information about them, whether or not we know it, whether or not we like it.

Is our resistance to these encroachments a quaint holdover from times before the great sweeps of digital technologies or does it reflect a genuine and legitimate sense of loss? And if there is a loss, what exactly is its nature and when is it worth fighting over rather than capitulating for the other benefits that these socio-technical practices promise?

These are the questions that have concerned me as I follow the inevitable debates accompanying newly introduced socio-technical practices, controversial because of their perceived threat to privacy. One might think that philosophical theories would provide important insights. To some extent they do. Their accounts of the nature of privacy, such as control over information about oneself, control over private information, or a limit on access to information about oneself, and explanations of why it ought to be cherished as a value in any liberal democracy, provide general ways to think about why these systems are *prima facie* problematic. The trouble with these theories is that they tend to be of limited use in resolving many of the most urgent problems, because the socio-technical practices in question do not merely threaten or violate privacy, they usually, at the same time, provide some benefit. Many philosophical theories leave us in the lurch, so to speak, when we drill down to these real world conflicts, and what tends to fill the gap instead is a struggle among stakeholders—and a free-for-all of preferences—over policies that serve their respective interests best.

The principle of contextual integrity provides guidance for privacy problems in the real world by highlighting not only morally and politically relevant changes brought about by socio-technical systems, but by providing a framework for interpreting the meaning and importance of these changes. It does so by introducing into the picture two theoretical constructs: contexts and informational norms.

Overview of Contextual Integrity

Contextual integrity is a philosophical account of privacy in terms of the transfer of personal information. It is not proposed as a full definition of privacy, but as a normative model, or framework, for evaluating the flow of information between agents (individuals and other entities), with a particular emphasis on explaining why certain patterns of flow provoke public outcry in the name of privacy (and why some do not). The approach encompassed by contextual integrity recognizes the key role of intricate systems of social rules governing information flow; these systems of rules are the crucial starting place for understanding normative commitments to privacy. While contextual integrity is itself a relatively recent term, the idea of context-relative informational norms has been "in the air," recognized in various ways in the literature,

by philosophers James Rachels and Ferdinand Schoeman, for example, and manifest quite concretely in rules of confidentiality governing the practice of many of the most prominent professions including law and medicine. Key elements of the theory of contextual integrity include: contexts, informational norms, appropriateness, roles, and principles of transmission.

With the concept of a context we intend to capture the idea that people act and transact in society not simply as individuals in an undifferentiated social world, but as individuals in certain capacities (roles), in distinctive social contexts, such as health care, education, employment, the marketplace, and so on. These contexts should be understood as structured settings whose features have evolved over time—sometimes long periods of time—a product not only of human intention but, additionally, a host of contingencies of place, culture, historical events, and more. Characteristic features of any context include the assemblage of roles (sometimes open-ended) and a set of behavior-guiding norms that prescribe (and proscribe) actions and practices. One further feature that is key to understanding "contexts", are ends, values, or purposes.

Consider how these characteristic features manifest themselves in a few mundane cases. In a healthcare context, of a physician's office, for example, roles may include those of patient, physician, nurse, receptionist, and bookkeeper. In the educational context of a school, we expect to find students, teachers, principals, and guidance counselors. In the commercial marketplace of a store, roles might include consumers, sales assistants, floor managers, stocking personnel, and store owners. For each of these roles certain behaviors, and certain responses to these behaviors are prescribed or expected. Of course, this does not mean that each move is prescribed by context relative norms; some contexts might prescribe only a few basic behaviors with the rest somewhat open-ended.

Roles and norms, however, are only part of what makes a context what it is. Were a visitor from outer space sent to earth to investigate social life on our planet, and, reporting on a typical healthcare setting of, say, a hospital, describe only the various roles and typical and expected behaviors, his audience would be unable to make proper sense of the goings-on. The activities in a hospital are meaningful, on the whole, only in relation to the underlying purposes of healthcare, generally, and a hospital, specifically, namely that of alleviating illness and promoting health. Although settling the exact nature of the ends and values for any given context is not a simple matter—even in the case of health care, which is relatively robust—the central point is that the roles and norms of a context make sense, largely, in relation to them.

In relation to privacy, the norms that interest us most are those governing the transmission of personal information, that is, those prescribing (and proscribing) the flow (or communication) of personal information from one party to another. These norms, which we call "informational norms," are singularly important. In a health care context, for example, informational norms prescribe what patients say to their physicians and limit what physicians can say to others about the health condition of patients under their care. Informational norms govern what shoppers need to communicate to sales clerks and what to fellow shoppers, and vice versa. Similarly, norms govern what teachers can ask about their students, what they are expected to say to their students' parents, and what they are not. Contextual integrity is a feature of situations in which context relative informational norms are respected; when informational norms have been unjustly breached, than we say that contextual integrity has been violated.

We have discussed informational norms in the most general terms, as rules guiding the flow of personal information from one party to another. There is more to say, however, about the internal structure of informational norms. One element of this structure is the information type (category, nature, class), the attribute or set of attributes that a particular norm governs. Whereas

many other prominent accounts of privacy acknowledge a simple dichotomy of information types—public and private (sensitive or intimate)—we have argued elsewhere that this dichotomy is problematic for the purpose of understanding a right to privacy. The theory of contextual norms, by contrast, posits a potentially indefinite array of types of information (attributes) that might feature in the informational norms of a given context. Appropriate is a term that seems intuitively well suited to the task of signaling whether information transmitted conforms to the requirement of informational norms. Consider how one might convey when discussing a job interview for the position of bank manager in the present-day United States. One might remark that it was *inappropriate* for the personnel officer to inquire about ones marital status. The same inquiry in the context of dating (or courtship) would be deemed appropriate. (Because information type is so salient an influence on people's judgments that a violation has occurred, earlier accounts of contextual integrity had posited norms of appropriateness as distinct from norms of transmission. Later efforts to formalize contextual integrity revealed that both factors featured in equivalent ways as parameters of informational norms.)

A second key element of informational norms is the actors or agents, reflecting the importance of a context's roles in determining people's rich and complex sensibilities about what information flows are acceptable. Associated with every communication, or transmission of information, there are three relevant agents: the one from whom the information flows, the one to whom the information flows, and the one—the information subject—about whom the information is. (There might be more than one individual associated with any of these agents.) What matters is the capacity, or role, in which an agent is acting, articulated with varying degrees of detail across and within contexts. In academic departments, for example, the roles of chair, tenured faculty, assistant professor, student, administrator, and so forth, are associated with specific, but sometimes roughly articulated, sets of duties and privileges, including some that apply to the flow of personal information.

A third key element of informational norms is the transmission principle, probably the most distinctive aspect of the theory of contextual integrity. Transmission principles govern the specific constraints (terms or conditions) regulating the flow of information from actor to actor. One such principle is confidentiality. If the informational norm specifies a principle of confidentiality, this means that it prohibits the agents receiving information from sharing it with others in the future. Confidentiality is one of the most salient of the transmission principles, but there are many other principles, for example, reciprocity, determining that information flow is bi-directional—occurring in friendship but not, say, between a patient and a physician. Another principle is desert, determining that an agent deserves to know or learn something about the information subject; perhaps, we might say, people might deserve to know whether their lovers are HIV positive.

Another important family of transmission principles hinges on the degree of awareness an information subject has about a particular flow, and whether the subject has a right of consent. Imagine, in one scenario, a person being questioned under oath in a court of law. Consent is not a reigning principle, but something more like compulsion. In another scenario, say deciding on the placement of video surveillance cameras in a public park, an important question might be whether subjects need to be aware that images are being captured. And, there are numerous scenarios in which the prescribed transmission principle is consent, in which case, information flows only when the consent constraint is satisfied. It is worth noting that control by subjects of the flow of information about themselves, which features definitively in certain theories, is merely one transmission principle—albeit an important one—among many. There is probably no end to the variation in transmission principles.

Contextual Integrity as a Heuristic

The value of contextual integrity in thinking through disputed practices is that it brings to light factors that are frequently not registered, or perceived, by other conceptions of privacy. It functions as a heuristic for determining why a given practice arouses indignation, resistance or protest, typically, by bringing to light a way or ways in which the practice violates entrenched informational norms. Consider the argument that RFID-enabled road toll plazas pose no new privacy threats because drivers are already out in public for all to see, applying the heuristic of contextual integrity reveals something different. Toll collectors accepting cash payments did not know who the drivers were, and with no systematic collection of license plate numbers there could, at best, be only transitory, fragmentary recollections of a vehicle type, color, number of travelers, and approximate time of day. And this knowledge would be locally rooted. These flows, as characterized by type of information, actors, and transmission principles look very different from those mapped when an RFID transponder tag relays a vehicle identity number to a transceiver in the plaza, in turn connected to a database of past transactions and credit card information; the information is complete, permanently recorded, stored in a central repository, and accessible to many others besides the toll collector and the car behind you under a range of possible terms. There are, no doubt, various reasons why practices, enabled by newly deployed socio-technical systems, raise objections. One, however, is that a new practice violates contextual integrity in ways sometimes undetectable via other approaches to privacy. The heuristic guides an analysis to ascertain the governing context and then to establish what changes the new practice has brought about in the types of information, the sender, recipient and subject of information, and the principles under which information is transmitted.

Is Contextual Integrity Inherently Conservative?

Even if one is convinced about the value of a social analysis of the kind proposed here, a legitimate concern is its reliance on past practice. Because contextual integrity is a measure of change and seems to imply change is bad, it is inherently conservative. There is validity to this charge, but it is justified only to a degree. I frame the situation in this way. Although the heuristic helps detect, it does not lead us automatically to reject change, only to be suspicious of it. Violation of contextual integrity is a warning signal, an explanation of why a change provokes anxiety. Yet, even as the theory's conservative stance impels us to investigate change, it also directs to interrogate, evaluate, and sometimes to embrace change.

As conduits for the capture, manipulation and dissemination of personal information, technologies and digital media promise great benefits to humanity at the same time as they pose an unfathomable threat to privacy. The best we can hope for is to hone our powers of discernment; to tell apart these potentialities, to evaluate them, to choose between them, and, where needed, to frame tradeoffs. Contextual integrity does not glibly address these needs; however it offers a systematic approach to unraveling what is at stake. In the first instance are cases when simply revealing an alternation in flows is sufficient to reverse or mitigate it. In the rest, we must consider the merits. Many thoughtful accounts of privacy have educated us on the value of privacy, explaining how it protects against harm, promotes individual freedom and autonomy, and social justice, equality, and democracy. But when should these prevail against considerations such as efficiency, safety and security, private property, and accountability, particularly when the benefits do not accrue equally to all sectors and all individuals in a society?

In the limited space remaining, I can offer only the barest sketch. First, is to maintain the focus of analysis at the contextual layer and to introduce into the picture contextual values, ends, and purposes. Second, is to notice that norms of information flow are not arbitrary (although often contingent); they serve the important function, frequently, of promoting substantive contextual ends. A quick example: the principle of confidentiality plays a crucial role in the medical context, as a person afflicted with a socially stigmatized condition might not otherwise seek medical care. This harms the one afflicted but, in the case of sexually transmitted diseases, poses a general threat to community health.

A more complex case is the context of political citizenship in a democracy. During elections, the intricate system of rules for assuring a secret ballot not only protects the rights of individuals, but promotes the democratic value (a contextual value) of equal voice: rich or poor, CEO or mail clerk, tyrant or oppressed, your vote counts the same as any other citizen's in this context, however uneven your stature in others. The same norms, however, do not govern congress, or houses of parliament where people acting in the capacities of representatives must cast their votes openly. It is conceivable that open voting subjects representatives to some of the same pressures from which a political community protects its individual citizens. One could argue, however, that in this case the values or ends of open government and accountability trump the dangers of intimidation, vote buying, and so forth.

Changes in practice that, for example, threaten the confidentiality of medical information or weaken the secrecy of individual ballots, may undermine the attainment of contextual ends. Whatever benefits are promised by the changes, this potential must weigh heavily against them. In other words, considerations are not merely who is harmed and who benefits, who is weakened and who empowered, but how the delicate balance that has evolved in a context, supported by an intricate system of norms, including but not limited to informational norms, might be disturbed or distorted by a particular change.

In established, ages-old contexts like medical care and democratic citizenship, we are well guided by history and experience. In contexts that themselves are newer, or at least, *prima facie,* seem newer, such as the context in which people conduct Web searches, this process involves greater challenges, including, for one, determining the nature of the context. These cases ought not discourage us from applying the framework of social analysis generally, and contextual integrity specifically, to defining substantive responses to them. On the contrary, the framework reveals the ways privacy is enmeshed in the problems of the larger worlds of society and politics; its problems often as messy and intractable.