Dædalus

Fall 2011: Protecting the Internet as a Public Commons

Dædalus

Journal of the American Academy of Arts & Sciences

Fall 2011

Protecting the Internet as a Public Commons

A Contextual Approach to Privacy Online

Helen Nissenbaum

Abstract: Recent media revelations have demonstrated the extent of third-party tracking and monitoring online, much of it spurred by data aggregation, profiling, and selective targeting. How to protect privacy online is a frequent question in public discourse and has reignited the interest of government actors. In the United States, notice-and-consent remains the fallback approach in online privacy policies, despite its weaknesses. This essay presents an alternative approach, rooted in the theory of contextual integrity. Proposals to improve and fortify notice-and-consent, such as clearer privacy policies and fairer information practices, will not overcome a fundamental flaw in the model, namely, its assumption that individuals can understand all facts relevant to true choice at the moment of pair-wise contracting between individuals and data gatherers. Instead, we must articulate a backdrop of context-specific substantive norms that constrain what information websites can collect, with whom they can share it, and under what conditions it can be shared. In developing this approach, the paper warns that the current bias in conceiving of the Net as a predominantly commercial enterprise seriously limits the privacy agenda.

HELEN NISSENBAUM is Professor of Media, Culture, and Communication and Senior Fellow in the Information Law Institute at New York University. Her books include *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2010), *Academy & the Internet* (edited with Monroe E. Price, 2004), and *Computers, Ethics & Social Values* (edited with Deborah G. Johnson, 1995).

The year 2010 was big for online privacy.[1] Reports of privacy gaffes, such as those associated with Google Buzz and Facebook's fickle privacy policies, graced front pages of prominent news media. In its series "On What They Know," *The Wall Street Journal* aimed a spotlight at the rampant tracking of individuals for behavioral advertising and other reasons.[2] The U.S. government, via the Federal Trade Commission (FTC)[3] and the Department of Commerce,[4] released two reports in December 2010 depicting the Net as a place where every step is watched and every click recorded by data-hungry private and governmental entities, and where every response is coveted by attention-seekers and influence-peddlers.[5]

This article explores present-day concerns about online privacy, but in order to understand and explain on-the-ground activities and the anxieties they stir, it identifies the principles, forces, and values behind them. It considers why privacy online has been vexing, even beyond general concerns over privacy; why predominant approaches have persisted de-

spite their limited results; and why they should be challenged. Finally, the essay lays out an alternative approach to addressing the problem of privacy online based on the theory of privacy as contextual integrity. This approach takes into consideration the formative ideals of the Internet as a public good.[6]

Setting aside economic and institutional factors, challenges to privacy associated with the Net are similar to those raised in the past by other information systems and digital media due to their vast capacities for capturing, stockpiling, retrieving, analyzing, distributing, displaying, and disseminating information. In a flourishing online ecology, where individuals, communities, institutions, and corporations generate content, experiences, interactions, and services, the supreme currency is information, including information about people. As adoption of the Internet and Web has surged and as they have become the primary sources of information and media for transaction, interaction, and communication, particularly among well-off people in technologically advanced societies, we have witnessed radical perturbations in flows of personal information. Amid growing curiosity and concern over these flows, policy-makers, public-interest advocates, and the media have responded with exposés and critiques of pervasive surreptitious tracking, manipulative behavioral advertising, and fickle privacy commitments of major corporate actors.

In *Privacy in Context: Technology, Policy, and the Integrity of Social Life*,[7] I give an account of privacy in terms of expected flows of personal information, modeled with the construct of *context-relative informational norms*. The key parameters of informational norms are actors (subject, sender, recipient), attributes (types of information), and transmission principles (constraints under which information flows). Generally, when the flow of information adheres to entrenched norms, all is well; violations of these norms, however, often result in protest and complaint. In a health care context, for example, patients expect their physicians to keep personal medical information confidential, yet they accept that it might be shared with specialists as needed. Patients' expectations would be breached and they would likely be shocked and dismayed if they learned that their physicians had sold the information to a marketing company. In this event, we would say that informational norms for the health care context had been violated.

Information technologies and digital media have long been viewed as threatening to privacy because they have radically disrupted flows of personal information, from the corporate and governmental databases of the 1960s to the surveillance cameras and social networks of the present day. The Net, in particular, has mediated disruptions of an unprecedented scale and variety. Those who imagined online actions to be shrouded in secrecy have been disabused of that notion. As difficult as it has been to circumscribe a right to privacy in general, it is even more complex online because of shifting recipients, types of information, and constraints under which information flows. We have come to understand that even when we interact with known, familiar parties, third parties may be lurking on the sidelines, engaged in business partnerships with our known parties. Information about us that once may have languished in dusty file cabinets is now pinpointed in an instant through search queries by anyone anywhere. In these highly *informatized* (that is, information-rich) environments, new types of information infuse our every action and relationship.

We are puzzled by the new and different types of information generated online, some of it the by-products of our activi-

ties, including cookies, latencies, clicks, IP addresses, reified social graphs, and browsing histories. New and different principles govern the flow of information: information we share as a condition of receiving goods and services is sold to others; friends who would not violate confidences repost our photographs on their home pages; people around the world, with whom we share nonreciprocal relationships, can see our houses and cars; providers from whom we purchase Internet service sell access to our communications streams to advertisers. Default constraints on streams of information from us and about us seem to respond not to social, ethical, and political logic but to the logic of technical possibility: that is, whatever the Net allows. If photographs, likes and dislikes, or listings of friends pass through the servers of a Facebook application, there is no telling whether they will be relinquished; if an imperceptible (to the ordinary user, at least) JavaScript code, or "beacon," is placed by a website one visits and enables the capture of one's browser state, so be it; if Flash cookies can cleverly work around the deletion of HTTP cookies, no harm done.

The dominant approach to addressing these concerns and achieving privacy online is a combination of *transparency and choice*. Often called notice-and-consent, or informed consent, the gist of this approach is to inform website visitors and users of online goods and services of respective information-flow practices and to provide a choice either to engage or disengage. Two substantive considerations explain the appeal of this approach to stakeholders and regulators. One is the popular definition of a right to privacy as a right to control information about oneself. Transparency-and-choice appears to model control because it allows individuals to evaluate options deliberately and then decide freely whether to give or withhold consent. How well it actually models control is not a question I pursue here because whatever the answer, there remains a deeper problem in defining a right to privacy as a right to control information about oneself, as discussed at length in *Privacy in Context*.[8]

A second consideration is the compatibility of notice-and-consent with the paradigm of a competitive free market, which allows sellers and buyers to trade goods at prices the market determines. Ideally, buyers have access to the information necessary to make free and rational purchasing decisions. Because personal information may be conceived as part of the price of online exchange, all is deemed well if buyers are informed of a seller's practices collecting and using personal information and are allowed freely to decide if the price is right. The ideal market assumes free and rational agents who make decisions without interference from third parties, such as government regulators. Doing so not only demonstrates respect for key actors, but also allows the market to function efficiently, producing the greatest overall utility.

However, there is considerable agreement that transparency-and-choice has failed.[9] Privacy advocates, popular media, and individuals have become louder and more insistent in pointing out and protesting rampant practices of surreptitious as well as flagrant data gathering, dissemination, aggregation, analysis, and profiling; even industry incumbents and traditionally pro-business government regulators admit that existing regimes have not done enough to curb undesirable practices, such as the monitoring and tracking associated with behavioral advertising and predatory harvesting of information posted on social networking sites. Why exactly the existing transparency-and-choice, or notice-and-consent,

approach has failed – and what to do about it – remains hotly disputed.

For many critics, whom I call *critical adherents*, the fault lies with the ubiquitous regime of offering privacy to individuals on a "take it or leave it" basis. A range of thoughtful commentaries on the subject, including those in the FTC and Department of Commerce reports mentioned above, have drawn attention to weak instantiations of choice, while others have highlighted problems with notice.[10] Because to choose means to deliberate and decide freely, the near-universal practice of modeling choice as "opt out" can hardly be said to model the ideal consumer making purchasing decisions in the ideal competitive marketplace. A deeper ethical question is whether individuals indeed freely choose to transact – accept an offer, visit a website, make a purchase, participate in a social network – given how these choices are framed as well as what the costs are for choosing not to do so.[11] While it may seem that individuals freely choose to pay the informational price, the price of not engaging socially, commercially, and financially may in fact be exacting enough to call into question how freely these choices are made.

Privacy policies as enactments of notice fare no better. That almost all privacy policies are long, abstruse, and legalistic adds to the unrealistic burden of checking the respective policies of the websites we visit, the services we consider and use, and the content we absorb. Compounding the burden is an entity's right to change its policy at will, giving due notice of such change, ironically, within the policy itself and therefore requiring interested individuals to read it not once but repeatedly. Unsurprisingly, ample evidence reveals that people do not read privacy policies, do not understand them when they do,[12] and realistically could not read them even if they wanted to.[13] This is not merely a matter of weakness of the will.

For critical adherents to transparency-and-choice, these observations point to the need for change, but not revolution. Such critics have suggested correctives including better mechanisms for choice, such as reframing policies in terms of "opt in" rather than "opt out" and locating moments of choice at times when users might be able to pause and think. They also advocate increasing transparency: for example, stipulating shorter policies that are easier to follow, along the lines of nutritional labels. Suggestions also apply to the content of policies. Whereas in the past, online actors were entreated simply to have policies, current correctives would require adherence to fair information principles.[14] The details of these suggestions are beyond the scope of this essay, as are questions about how privacy policies and practices should be monitored and enforced. This is because (as I argue below) the consent model for respecting privacy online is plagued by deeper problems than the practical ones noted so far.

I am not convinced that notice-and-consent, however refined, will result in better privacy online as long as it remains a procedural mechanism divorced from the particularities of relevant online activity. Take the example of online behavioral advertising, which quickly reveals an inherent flaw with the notice-and-consent approach.[15] To begin, consider what might need to be conveyed to users to provide notice of what information is captured, where it is sent, and how it is used. The technical and institutional story is so complicated that probably only a handful of deep experts would be able to piece together a full account; I would hazard that most of the website owners who contract with ad networks providing targeted advertising services are not among such experts. Even if,

for a given moment, a snapshot of the information flows could be grasped, the realm is in constant flux, with new firms entering the picture, new analytics, and new back-end contracts forged: in other words, we are dealing with a recursive capacity that is indefinitely extensible.[16] As a result of this complex and shifting landscape, users have been prone to conflate (in a convenient but misleading way) tracking with targeting. Further, the complexity makes it not only difficult to convey what practices are followed and what constraints respected, but practically impossible.[17]

For critical adherents to notice-and-consent, these types of cases exemplify the need for brief and clear policies that capture the essence of privacy practices in ways ordinary people can grasp. I view this as a futile effort because of what I call the *transparency paradox*. Achieving transparency means conveying information-handling practices in ways that are relevant and meaningful to the choices individuals must make. If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference: who are the business associates and what information is being shared with them; what are their commitments; what steps are taken to anonymize information; how will that information be processed and used. An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance.[18] Thus the transparency paradox: transparency of textual meaning and transparency of practice conflict in all but rare instances.[19] We seem unable to achieve one without giving up on the other, yet both are essential for notice-and-consent to work.

Adherents may persist, pointing to other arenas, such as health care and human subject research, in which a similar transparency paradox appears to have been overcome. In health care, informed consent protocols are commonly accepted for conveying risks and benefits to patients undergoing surgery, for example, or to subjects entering experimental treatment programs, even though it is unlikely they fully grasp the details. In my view, these protocols work not because they have found the right formulation of notice and the authentic mechanism for consent but because they exist within a framework of supporting assurances. Most of us are terrible at assessing probabilities and understanding risks of side effects and failed procedures; we are extremely poor at visualizing the internal organs of our bodies. It is not the consent form itself that draws our signature and consigns us to the operating table, but rather our faith in the system.[20] We trust the long years of study and apprenticeship that physicians undergo, the state and board certifications, peer oversight, professional codes, and above all, the system's interest (whatever the source) in our well-being. We believe in the benevolence of institutions of higher learning and, in large part, their mission to promote human welfare. Far from perfect, and subject to high-visibility breaches, the systems that constitute these safety nets have evolved over centuries; they undergird and warrant the consent agreements that patients and subjects confront every day. In the online environment, by contrast, individual consent agreements must carry the entire weight of expectation.

Picking holes in the transparency-and-choice (informed consent) approach, problematic as it is, is not the end point of

my argument. As it is, it may be the best approach for this interim period while the supporting assurances to shore it up are developed. Such assurances are not achieved by fiat, but may require decades for relevant institutional forms and practices to progress from trial and error to a balanced settling point. The theory of contextual integrity offers a shorter and more systematic path to this point by invoking learned wisdom from mature systems of informational norms that have evolved to accommodate diverse legitimate interests as well as general moral and political principles and context-specific purposes and values. The promise of this path is not merely that the equilibriums achieved in familiar contexts may provide analogical guidance for online realms; rather, the path acknowledges how online realms are inextricably linked with existing structures of social life. Online activity is *deeply integrated* into social life in general and is *radically heterogeneous* in ways that reflect the heterogeneity of offline experience.

By now, the story is familiar: about the advent of ARPANET and, out of this, the Internet, email as the unanticipated "killer app," the handoff of management from government to private industry, and emergence of the Web as the dominating platform for most ordinary people's experience of the Net. Along the way, the Internet has progressed from an esoteric utility for sharing computer resources and data sets, intended for use by relatively few specialists, to a ubiquitous, multifunctional medium used by millions worldwide.[21] As it has progressed through these stages, it has been conceptualized through a series of influential ideations:[22] from information superhighway,[23] enabling swift flows of information and commerce;[24] to cyberspace, a new frontier immune from the laws of any land; to Web 2.0, a meeting place overflowing with services and content, much of it generated by users themselves.[25]

Each of these ideations captured salient aspects of the vast socio-technical system that I have been calling "the Net" as it developed through progressive phases, and as it continues to do so today. Indeed, the Net is characterized by enormous malleability, both over time and across applications. Although the brute technical substrate of digital media – architecture, design, protocol, feature sets – may constrain or afford certain activities, it does so no more than, say, gravitational force, which similarly constrains and affords human activity while leaving plenty of room for variation. For example, the Net may have seemed *essentially* ungovernable until China asserted control and territorial borders quietly reemerged. Yet even that maneuver is incomplete, leaving intact exhilarating pockets of autonomy.[26]

A snapshot of today's Net, conceived as an abstraction of technical layers and social (economic and political) systems, operates as infrastructure, bustling spaces, and medium. Whether "online," "in cyberspace," "on the Internet," or "on the Web," individuals engage in banal practices such as banking, booking travel, and shopping, in many instances doing so with the same institutions and companies they could call on the telephone or visit at a physical location. Other activities – viewing movies, listening to recordings, reading literature, talking on an IP phone, seeking information, communicating via email, worshipping, and some forms of shopping – are transformed in their migration to the Net. In many instances, these transformations are not merely experiential but reflect institutional innovations, such as online churches and dating services, virtual universities, websites such as Amazon, Netflix, Mayo Clinic, WebMD, eBay, and E*TRADE, and

programs and services such as e-government, e-zines, e-vites, e-readers, iTunes, and iShares.

Even greater novelty and more fundamental transformations are found in the activities, practices, and institutional and business forms built on top of these offerings, including meta-engines that aggregate, index, organize, and locate sites, services, goods, news, and information; examples include kayak.com, Google search, Google news, and Yelp.com. Web 2.0 has wrought an additional layer of changes, notably in production, creativity, and social life. These changes include interacting via social networks, networking on platforms, and facilitating peer-production and user-generated content by way of innumerable individual and small-group blogs, wikis, and personal websites; repositories of global scale such as Wikipedia, IMDb, Flickr, MMORGs (massively multiplayer online role-playing games), and YouTube; the online patient-support community PatientsLikeMe; as well as mash-ups, folksonomies, crowdsourcing, and reputational systems.

Questions about protecting privacy online, particularly when framed as questions about *online privacy*, suggest that "online" is a distinctive venue, sphere, place, or space defined by the technological infrastructures and protocols of the Net, for which a single set of privacy rules can, or ought to, be crafted. I resist this notion. However exhilarating the vision of cyberspace as a new frontier, experience reveals no insulated domain divorced from "real life" and deserving distinctive regulation. The Net does not constitute (drawing on the terminology of contextual integrity) a discrete context. It is not a single social realm, but the totality of experience conducted via the Net, from specific websites to search engines to platforms and on up into "the cloud," crisscrossing multiple realms. Activities online, mediated by the Net ("on" the Web), are deeply integrated into social life: they may be continuous with brick-and-mortar correlates or, at the very least, have the power to affect communications, transactions, interactions, and activities in those realms (and vice versa). Not only is life online integrated into social life, and hence not productively conceived as a discrete context, it is *radically heterogeneous*, comprising multiple social contexts, not just one, and certainly is not just a commercial context where protecting privacy amounts to protecting *consumer* privacy and commercial information.[27] To be sure, the contours of technology (architecture, protocol, design, and so on) shape what you can do, say, see, and hear online, but while alterations, or disruptions due to particular characteristics of the Net, impose puzzles and pose challenges for social contexts, they do not warrant sui generis, uniform, cross-cutting rules determined by the medium. Instead, the contexts in which activities are grounded shape expectations that, when unmet, cause anxiety, fright, and resistance.[28]

Answering questions about privacy online, like those about privacy in general, requires us to prescribe suitable, or appropriate, constraints on the flow of personal information. The challenge of privacy online is not that the venue is distinct and different, or that privacy requirements are distinct and different, but that mediation by the Net leads to disruptions in the capture, analysis, and dissemination of information as we act, interact, and transact online. The decision heuristic derived from the theory of contextual integrity suggests that we locate contexts, explicate entrenched informational norms, identify disruptive flows, and evaluate these flows against norms based on general ethical and political principles as well as context-specific purposes and values.

To be sure, locating *contexts online* and explicating the *presiding norms* is not always straightforward (in the same way that it is not when dealing with unmediated social spaces). Some of the more familiar cases, however, may provide insight into the task. Whether you transact with your bank online, on the phone, or person-to-person in a branch office, it is not unreasonable to expect that rules governing information will not vary according to medium. In the United States, banks and other financial institutions are governed by privacy rules formulated by the FTC, which was given this authority by the Gramm-Leach-Bliley Act.[29] Auxiliary information (for example IP address or clickstream), the artifacts of online transaction, should not simply be deemed "up for grabs" just because that information was not explicitly considered in rules formulated before online banking became common. Instead, it should be held to the same standards that guided financial privacy in the first place.

Similarly, while expectations of visitors to Bloomingdales.com, NYTimes.com, and MOMA.org may be affected by corresponding, preexisting brands, they are also shaped by the respective social contexts that these entities inhabit, including the types of experiences and offerings they promise. Accordingly, Amazon.com, which came on the scene as an online bookstore with no brick-and-mortar precursor, is nevertheless recognizable, akin to, say, the Moravian Book Shop in Bethlehem, Pennsylvania, which was founded in 1745 and is believed to be the oldest continually operating bookstore in the United States.[30] As Amazon.com expanded into other arenas, selling and renting DVDs, for example, one would assume personal information flows generated in these transactions to be regulated by constraints expressed in the Video Privacy Protection Act of 1988[31] in the same way that West Coast Video must adhere to the Act. Whether laws applicable to brick-and-mortar video rental stores actually apply to online video rental providers such as iTunes and Amazon seems uncertain; still, the requirements of contextual integrity, which anchors privacy rules in social contexts and social roles, would imply that they should.

These examples merely scratch the surface of the Net's remarkable heterogeneity. Online offerings range from specialized information providers and distributors, such as MayoClinic.com and WebMD; federal, state, and local government portals, providing services and information directly to citizens; and structured repositories of user-generated content, such as Wikipedia, YouTube, Flickr, Craigslist, and social networks, including Facebook. Religious denominations around the globe have online presences, ranging from The Holy See, claiming to be the "official" Vatican website,[32] to online churches,[33] offering in-home, Web-based religious engagement that replaces or supplements regular church attendance. This list does not capture the fluidity and modularity of existing offerings, which include combinations and permutations (mash-ups) constrained only by human creativity and the technological limits of the moment. Many popular websites, for example, combine modules of enterprise-generated content with user-generated feedback, or storefronts with varieties of social networks, political content with open blogs, and more.

To the extent that the Net is deeply embedded in social life, context-specific informational norms may be extended to corresponding online activities. Thus, privacy rules governing financial institutions, for example, would extend to E*TRADE even though it operates primarily via an online portal. Online offerings and experiences may defy existing norms, how-

ever, as they incorporate some of the novel forms mentioned above. In such circumstances, the theory of contextual integrity directs us beyond existing norms to underlying standards, derived from general moral and political considerations as well as the ends, purposes, and values of respective contexts.[34] Novel activities and practices, which implicate different types of information, expanded groups of recipients, and altered constraints on flow are evaluated against these standards.

Applying this reasoning to online filing of income tax returns is fairly straightforward. In the United States, rigorous confidentiality requirements governing individual tax records, impervious even to certain types of law enforcement needs, have developed over the past 150 years.[35] Although present-day code, formalized in the 1970s, may have little to say about e-filing specifically, we would not expect auxiliary information generated through online interactions to be "up for grabs," freely available to all comers. Even in the absence of explicit rules, guidance can be sought from the values and purposes that have yielded existing confidentiality rules for information in traditional paper-based tax records. In the Disclosure and Privacy Law Reference Guide, the IRS asserts that "there must be public confidence with respect to the confidentiality of personal and financial information given to us for tax administration purposes. . . . The confidential nature of these records requires that each request for information be evaluated in light of a considerable body of law and regulation which either authorize or prohibit disclosure."[36] This connection was acknowledged as far back as 1925, when Secretary of the Treasury Andrew Mellon remarked, "While the government does not know every source of income of a taxpayer and must rely upon the good faith of those reporting income, still in the great majority of cases this reliance is entirely justifiable, principally because the taxpayer knows that in making a truthful disclosure of the sources of his income, information stops with the government. It is like confiding in one's lawyer."[37] A presumption of strict confidentiality is derived from values and purposes – public compliance, trust, confidence in government – that prohibit all sharing except as allowed, on a case-by-case basis, by explicit law and regulation.

The more challenging cases confronting us include forms of content, service, and interaction that are specific to the Net or that do not have obvious counterparts elsewhere. Search engines such as Google and Bing, essential for navigating the Web, may constitute an important class of cases. And while sites such as Mayo Clinic and WebMD might seem similar enough to familiar reference resources, health information sites are prodigious,[38] offering everything from personalized and interactive services that allow users to sign in and pose questions about their particular problems, to personal health record repositories that provide space to store health records (for example, Microsoft Health Vault), and to social networking sites devoted to communities of fellow sufferers (for example, PatientsLikeMe).

Without denying that the Net has yielded much that is novel and strange, including new types of information and new institutional forms, online activities themselves are strangely familiar: connecting with a friend, collaborating on a political mission, applying for a job, seeking religious or spiritual sustenance, pursuing educational opportunity, catching up on local and world news, or choosing a book to read, music to enjoy, or movies to watch. Although searching on Google is different from looking up material in a library catalog, in part because the contents of the

Web are quite different from the contents of a library, there is similarity in these two activities: both may include the pursuit of research, knowledge, and intellectual enrichment. In all such activities, liberal democratic societies allow great freedom, unconstrained by the watchful gaze or approbation of authorities, just as they allow citizens to seek political or religious information or affiliation. Just as with the offline environment, we would expect the same standards to prevail online, dictating that online footprints should not be recorded and registered in order to minimize risk of interference, by either human or machine.

The interest in privacy online that the FTC and Commerce Department have recently shown is a positive development, particularly because it acknowledges a growing concern over privacy and amplifies public discussion of the wildly unrestrained collection of personal information by nongovernmental actors. Their interest has been limited, though, by a focus on protecting privacy online as, predominantly, a matter of protecting *consumers* online and protecting *commercial* information: that is, protecting personal information in commercial online transactions.[39] Neither agency has explicitly acknowledged the vast landscape of activity lying outside the commercial domain. As long as public discourse about privacy online takes the marketplace and commerce as proxies for the whole, conceptions of privacy will be inadequate. We need to take full account of the radical heterogeneity of online activity and practice.

One might argue that the Net *is* almost completely commercial, pointing to the prevalence of private payment as the means supporting online activity. Aside from government presences, the Net is almost wholly owned by private, for-profit entities, from the underlying physical infrastructure to network service providers, providers of utilities and applications, and retailers of goods, content, and services. Furthermore, commercial advertising managed through the complex ecosystem of ad networks, ad exchanges, and analytics and marketing companies has emerged as a dominant business model for supporting online content and services. This model prevails in a variety of online locations, from large corporate websites, to personal blogs such as Noob Cook, a site with seventeen trackers, or Dictionary.com, with nine trackers from advertising companies, such as Doubleclick, Media Math, Microsoft Atlas, and others.[40] Wikipedia remains a rather remarkable standout, supported by the nonprofit Wikimedia Foundation and sporting no trackers.[41]

By this logic, the Commerce Department and the FTC would be precisely the governing bodies to have oversight of online activity, and norms of the competitive, free marketplace would make the most sense for regulating it. Yet private payment, whether through direct charges for goods, services, access, or participation, or through income from advertising, does not on its own signal complete surrender to marketplace norms. According to political philosopher Elizabeth Anderson, many functions in society straddle boundaries between the commercial and noncommercial. How they are supported is not decisive but rather how they measure up to standards of quality or excellence. Private payment as a form of support does not require total concession to marketplace norms; instead, we expect functions such as education, health care, religion, telecommunication, and transportation, whether privately paid for or not, to meet independent ideals. As Anderson warns, "When professionals sell their services,

they enter into market relations that impose norms on their activities which potentially conflict with the norms of excellence internal to their professional roles."[42] But we expect more from professionals – from doctors, lawyers, athletes, artists, church ministers, and teachers – than the pursuit of profit. People pay for medical care at private practices and hospitals, for instance, and for education at a variety of institutions. In these and other cases, in which complete surrender to marketplace norms would result in corrupt and impoverished practice, Anderson advocates a proper balance of market norms with internal standards of excellence.

This point might seem obvious, but certain brands of free-market capitalism make it easy to confuse the quest for profit with the pursuit of internal standards of excellence.[43] When Sergey Brin and Larry Page first launched the Google search engine, they regarded commercial influences as contrary to a search engine's core mission as a performance-driven tool serving individuals' interests in locating information on the Web. Eschewing advertising, they wrote in the appendix of a 2007 paper, "The goals of the advertising business model do not always correspond to providing quality search to users. . . . We believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm."[44] In other, less visible cases, similar concerns may be raised: for example, Amazon's purchase of IMDb, a website of information about movies, developed and initially maintained by volunteers. Even in the case of the familiar lending library, originally conceived in the United States by Benjamin Franklin as publicly funded, many functions have been taken over by private, for-profit companies online.[45]

The point is not to see Brin and Page or other developers as "sellouts." Confounding sources of support with guiding norms obscures our recognition of the internal standards of excellence that we can hold search companies to even as they seek commercial support, independent of their performance in the marketplace.[46] The same argument holds for content vendors and information services providing, in the private sector, many services also provided by public libraries. I am not suggesting that there is consensus, or that questions about internal norms of excellence are easily settled; endless struggles over what constitutes a good newspaper, school, or health care system attest to this. But they also reveal a strong belief that beyond profit, such standards are at play and are socially important.

Recent attention given to the challenge of protecting privacy online is a positive development. Although success is hamstrung by the foot-dragging of those whose power and profit are served by unrestricted flows of personal information, it is also limited by underdeveloped conceptions of privacy and the role it plays in sustaining the Net as a public good, capable of serving diverse interests. Early portrayals of cyberspace as a new frontier, different, distinct, and out of the reach of traditional law, have for the most part been abandoned, yet no other single vision has captured public imagination in quite the same way. This is unsurprising given the Net's massive growth as a complex infrastructure, content delivery system, and media space. The lack of a reigning public vision has meant that controversial moral and political matters are settled more often by technical affordances than by clearly articulated public moral and political principles. For privacy this has been devastating, as the Net, constructed

through an amalgamation of the sciences and technologies of information, computation, and networking, affords radical disruptions of information flows. With economic and social incentives stacked against constraints on flow, burdening individuals with the full weight of protecting their privacy online through notice-and-choice is unlikely to yield success.

My preferred alternative builds from the vision of life online as heterogeneous and thickly integrated with social life. Despite distinctive qualities of online movement, transactions, activities, relations, and relationships, when abstracted from particulars these retain fidelity with the fundamental organizing principles of human practice and social life. Drawing on work from social theory and philosophy, the framework of contextual integrity conceives of these spheres as partially constituted by norms of behavior, among them norms governing the flow (sharing, distributing) of personal information. We should not expect social norms, including informational norms, simply to melt away with the change of medium to digital electronic any more than from sound waves to light particles. Although the medium may affect what actions and practices are possible and likely, sensible policy-making focuses on the actions and practices themselves, with an eye to their function within social spheres and their standing in relation to entrenched social norms.

Two broad recommendations follow from the argument thus far. First, in our online activity we should look for the contours of familiar social activities and structures. For much that we do online – banking, shopping, communicating, and enjoying culture and entertainment – this is not a difficult task. Where correspondences are less obvious, such as consulting a search engine to locate material online, we should consider close analogues based not so much on similarity of action but on similarity of function or purpose. Consulting a search engine, in this regard, is akin to conducting research, seeking information and association, searching a library catalog, and pursuing intellectual enlightenment. Time spent on social networks, such as Facebook, is an amalgam of engagement with personal, social, intimate and home life, political association, and professional or work life. As we locate correspondences, we bring into view the relevant governing norms. If I am right about how search engines are used and for what purposes, then the governing norms would be strict confidentiality with regard to Web search histories and perhaps, as practiced by many public libraries, the prompt expunction of such records to minimize risks of leakage or mandated handovers as well as the temptation of future sharing for financial gain. At present, Google, unlike other search providers, has expressed a commitment to maintaining a barrier between identifiable search records and other records it accumulates with user profiles. Although this decision adheres to the spirit of the conception of Web search I have urged, questions remain about the efficacy of their approaches to de-identifying search logs and the fact that the commitment can be revoked at any moment, as was Google's commitment to forgo behavioral advertising.[47]

This view of online privacy also implies that contexts, not political economy, should determine constraints on the flow of information. Companies merge and acquire other companies for many different reasons: for example, to strengthen and expand their range of holdings, to gain market dominance in a particular area, or to establish control over vertical chains of necessary resources. Among the valu-

able assets that motivate acquisitions are databases of personal information, as demonstrated (presumably) by Google's acquisition of Doubleclick and Choicepoint's systematic acquisitions of smaller, special-purpose data holders.[48] But databases of personal information shared in one context, under constraints of the relevant informational norms, should not be treated as just another asset, akin to buildings, furniture, and supplies. The privacy policies of large diverse companies, such as Walt Disney, General Electric, Google, Citigroup, Viacom, and Microsoft, however, reveal porous boundaries among subsidiaries, with little acknowledgment of a need to account for patterns of information flow within a single company. Online conglomerates are no different as they strive to achieve vertical integration by controlling the raw materials of their industry, namely, information. Against these trends, we must establish respect for the boundaries of context and associated informational norms.

There is little doubt that when communicating with the public, corporations understand the importance of acknowledging the integrity of contexts. Even though to corporate investors a company might boast diverse informational assets, to the public it generally identifies units that are socially meaningful. It may be that in these acts of self-presentation, companies acknowledge the contextual heterogeneity of their offerings and therefore open the door to corresponding context-specific norms. By calling its online offering a university, a shoe store, a church, a medical center, a friendship network, or a bank, a company gives users a way to understand the services or activities that take place there, and it invites evaluation against respective norms, whether these are embodied in law or simply arise from reasonable expectations.[49] Staying true to these self-portrayals requires companies to commit to partitioning information holdings along contextual contours rather than along lines of corporate ownership.

There is no denying the transformative effects of digital technologies, including the rich and teeming online activity they have spawned. Recommending that we locate familiar social contexts online and, where it makes sense, connect activities and offerings with them is not to dispute this. Instead, the aim is to reveal relevant standards of excellence. As social contexts, activities, roles, and rules migrate online, respective context-specific values, ends, and purposes serve as standards against which information-sharing practices can be evaluated as legitimate or problematic. It is important to keep in mind that privacy norms do not merely protect individuals; they play a crucial role in sustaining social institutions.[50] Accordingly, restraints on search engines or social networks are as much about sustaining important social values of creativity, intellectual growth, and lively social and political engagement as about protecting individuals against harm. Benjamin Franklin knew as much when he insisted on privacy protection for the U.S. mail, not only to protect individuals but also to promote a meaningful social role for the service. We should expect no less for email and IP telephony.

My second recommendation applies to online cases without straightforward social precedents. As discussed earlier, social forms online sometimes enable configurations of actors, information, activities, and experiences that are unfamiliar, at least prima facie. In these cases, I suggest starting with ends, purposes, and values and working from there back to norms. A politician's website that allows citizens to "talk back" comprises an unusual platform for which no preexisting rules apply to, say, digital footprints left

by visitors to the site. Here, the right approach is not an opportunistic information grab. Although this may serve immediate needs of an imminent political campaign, it does not serve the purposes of encouraging frank political discussion, which is understood to flourish in environments of great freedom.[51] If people expect to be monitored, if they anticipate that their recorded views will be shared with particular third parties for money or favors, they are likely to be more watchful, circumspect, or uncooperative. The issue, however, is not how particular practices affect individuals, but the implications for particular purposes and values. Circumspection and cooperativeness are productive of certain ends but not others. Working backward from these values, we develop rules for situations in which there appear not to be any obvious candidates.

Growing momentum to confront the problem of privacy online is a welcome development. It would be a mistake, however, to seek remedies that make privacy online something distinct. Protecting privacy is a matter of assuring appropriate flows of personal information, whether online or offline, and disruptions in information flow, enabled by information technologies and digital media, can be equally disturbing, whether online or off. Because much of what happens online is thickly integrated with social life writ large (and vice versa), solving the privacy problem online requires a fully integrated approach. I have articulated one step toward this goal, resisting the suggestion that, with regard to privacy, the Net is virgin territory where it falls to the parties to construct terms of engagement for each transaction. Given how deeply rooted are our expectations of right and wrong concerning the sharing of information about ourselves and others, it is no wonder that over time intricate systems of norms have developed to govern all domains of social life.

To adapt these systems to social relations and contexts that have expanded into digital media spaces, we must make explicit much that has operated implicitly, and in the process reject entrenched norms that no longer promote the achievement of moral and political values as well as context-specific ends. To leave the protection of privacy online to negotiations of notice-and-consent is not only unfair, it is to pass up a critical public policy opportunity that will have ramifications for the shape and future of the Net. If pursued conscientiously, the process of articulating context-based rules and expectations and embedding some of them in law and other specialized codes will yield the safety nets that buttress consent in fields such as health care and research. With these precautions in place, plenty of room would still remain to express personal preferences and to maintain a robust role for informed consent.

ENDNOTES

[1] This essay has benefited from opportunities to present at the Center for Law, Technology, and Society, University of Ottawa; the Center for the Study of Law and Society, University of California, Berkeley; and the Center for Internet and Society, Stanford University, where questions and comments led to significant improvements and refinements of the argument. I am grateful for valuable feedback from David Clark and NYU's Privacy Research Group, expert guidance from Cathy Dwyer and Foster Provost, and sterling research assistance from Jacob Gaboury and Marianna Tishchenko. This work was supported by grants AFSOR: ONR BAA 07-03 (MURI) and NSF CT-M: Privacy, Compliance & Information Risk, CNS-0831124.

[2] Jennifer Valentino-Devries, "What They Know About You," *The Wall Street Journal*, July 31, 2010, http://online.wsj.com/article/SB10001424052748703999304575399041849931612.html.

[3] U.S. Federal Trade Commission, Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[4] U.S. Department of Commerce, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," December 2010, http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[5] Compare these depictions to earlier accounts of the Net as a new frontier of freedom and autonomy: for example, David R. Johnson and David G. Post, "Law and Borders – The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1367; John Perry Barlow, "Electronic Frontier: Coming into the Country," *Communications of the ACM* 34 (3) (March 1991).

[6] In this essay, I draw most of my examples from the World Wide Web because almost all the controversial privacy concerns that have captured public attention have stemmed from Web-based activity and because the online experiences of ordinary people occur mostly on the Web. I will use the term *Net* when observations made about the Web seem pertinent to other Internet applications and services.

[7] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, Calif.: Stanford University Press, 2010).

[8] Ibid., chap. 5.

[9] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change" and Department of Commerce, "Commercial Data Privacy and Innovation in the Internet Economy."

[10] Fred Cate, "The Failure of Fair Information Practice Principles," in *Consumer Protection in the Age of the "Information Economy,"* ed. Jane K. Winn (London: Ashgate Publishing, 2006).

[11] Ian Kerr, "The Legal Relationship Between Online Service Providers and Users," *Canadian Business Law Journal* 35 (2001): 1–40.

[12] Joseph Turow, Lauren Feldman, and Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline* (Philadelphia: Annenberg Public Policy Center, University of Pennsylvania, June 1, 2005), http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf.

[13] Lorrie Faith Cranor and Joel Reidenberg, "Can User Agents Accurately Represent Privacy Notices?" The 30th Research Conference on Communication, Information, and Internet Policy (TPRC2002), Alexandria, Virginia, September 28–30, 2002.

[14] U.S. Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July 1973, http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[15] Solon Barocas and Helen Nissenbaum, "On Notice: The Trouble with Notice and Consent," *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, Cambridge, Massachusetts, October 12–

13, 2009; Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, and Solon Barocas, "Adnostic: Privacy-Preserving Targeted Advertising," *Proceedings of the Network and Distributed System Symposium*, San Diego, California, February 28 – March 3, 2010.

16 Counting ad servers alone, a list current as of April 2011 shows 2,766 unique entries; see http://pgl.yoyo.org/adservers/formats.php (accessed April 13, 2011).

17 Barocas and Nissenbaum, "On Notice," and Toubiana, Narayanan, Boneh, Nissenbaum, and Barocas, "Adnostic."

18 Vincent Toubiana and Helen Nissenbaum, "An Analysis of Google Log Retention Policies," *The Journal of Privacy and Confidentiality* (forthcoming).

19 For example, personal information is shared with no one and destroyed after each session.

20 Deborah Franklin, "Uninformed Consent," *Scientific American*, March 2011, 24 – 25.

21 See Katie Hafner and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Simon and Schuster, 1999); Tim Berners-Lee, *Weaving the Web: The Past, Present and Future of the World Wide Web by Its Inventor* (London: Texere Publishing, 2000); and Janet Abbate, *Inventing the Internet* (Cambridge, Mass.: MIT Press, 2000).

22 On this transformation of the Internet through the "tussle" of interested parties, see David Clark, John Wroclawski, Karen Sollins, and Robert Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet," *Proceedings of the ACM SigComm 2002 Conference*, Pittsburgh, Pennsylvania, August 19 – 23, 2002, published in *Computer Communications Review* 32 (4) (October 2002).

23 Al Gore, "Infrastructure for the Global Village: Computers, Networks and Public Policy," special issue, "Communications, Computers, and Networks," *Scientific American*, September 1991, 150 – 153.

24 John Perry Barlow, "The Economy of Ideas," *Wired*, March 1994, 84.

25 Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin, 2009).

26 Samantha Shapiro, "Revolution, Facebook-Style," *The New York Times*, January 22, 2009, http://www.nytimes.com/2009/01/25/magazine/25bloggers-t.html.

27 Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," and Department of Commerce, "Commercial Data Privacy and Innovation in the Internet Economy."

28 Compare this notion to Mark Zuckerberg's claim that norms change due to the contours of Facebook's privacy policies; see Bianca Bosker, "Facebook's Zuckerberg Says Privacy No Longer a 'Social Norm,'" The Huffington Post, January 11, 2010, http://www.huffingtonpost.com/2010/01/11/facebooks-zuckerberg-the_n_417969.html.

29 U.S. Federal Trade Commission, Gramm-Leach-Bliley Act 15 U.S.C., Subchapter I, sec. 6801 – 6809, November 12, 1999, http://www.ftc.gov/privacy/glbact/glbsub1.htm; Adam Barth, Anupam Datta, John Mitchell, and Helen Nissenbaum, "Privacy and Contextual Integrity: Framework and Applications," *Proceedings of the IEEE Symposium on Security and Privacy*, Berkeley, California, May 21 – 24, 2006.

30 The Moravian Book Shop now has its own online portal, http://www.moravianbookshop.com/ (accessed April 13, 2011).

31 The Video Privacy Protection Act 18 U.S.C. sec. 2710, 1988, http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002710----000-.html.

32 See http://www.vatican.va/phome_en.htm (accessed April 13, 2011).

33 See http://www.online-churches.net (accessed April 13, 2011).

34 Nissenbaum, *Privacy in Context*, esp. chap. 8.

35 David Kocieniewski, "IRS Sits on Data Pointing to Missing Children," *The New York Times*, November 12, 2010, http://www.nytimes.com/2010/11/13/business/13missing.html.

36 Internal Revenue Service, "Disclosure and Privacy Law Reference Guide," Publication 4639 (10-2007) Catalog Number 50891P, 1–7.

37 Hearings on Revenue Revision 1925 Before the House Ways and Means Committee, 69th Cong., 1st sess. 8–9 (1925).

38 A Google search on "HIV status," performed January 11, 2011, yielded more than 7.5 million results.

39 Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," and Department of Commerce, "Commercial Data Privacy and Innovation in the Internet Economy."

40 Noob Cook is presented as being written by "a girl who likes to cook"; see http://www.noobcook.com/about/ (accessed February 25, 2011).

41 Establishing the number of trackers on a website is highly inexact. Various utilities offer this service, for example, Ghostery; numbers vary depending on the approaches they adopt. Not all approaches recognize all types of trackers. Further, these numbers also vary from time to time because websites may frequently revise their underlying policies and business arrangements. (I am indebted to Ashkan Soltani for clarifying this point.)

42 Elizabeth Anderson, *Value in Ethics and Economics* (Cambridge, Mass.: Harvard University Press, 1995), 147.

43 Milton Friedman, "Can Business Afford to be Ethical?: Profits before Ethics," in *Ethics for Modern Life*, ed. Raziel Abelson and Marie-Louise Friquegnon, 4th ed. (New York: St. Martin's Press, 1991), 313–318.

44 Sergey Brin and Lawrence Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," *WWW7/Computer Networks* 30 (1–7) (1998): 107–117; quotation taken from Web version, http://infolab.stanford.edu/~backrub/google.html (accessed February 26, 2011). See also Alex Diaz, "Through the Google Goggles: Sociopolitical Bias in Search Engine Design," in *Web Searching: Interdisciplinary Perspectives*, ed. Amanda Spink and Michael Zimmer (Dordrecht, The Netherlands: Springer, 2008).

45 Robert Ellis Smith, "Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet," *Privacy Journal* (2000): 34, 51.

46 Lucas Introna and Helen Nissenbaum, "Shaping the Web: Why the Politics of Search Engines Matters," *The Information Society* 16 (3) (2000): 1–17; Frank Pasquale and Oren Bracha, "Federal Search Commission? Access, Fairness, and Accountability in the Law of Search," *Cornell Law Review* 93 (2008): 1149; Toubiana, Narayanan, Boneh, Nissenbaum, and Barocas, "Adnostic."

47 Toubiana and Nissenbaum, "An Analysis of Google Log Retention Policies."

48 See "Choicepoint," EPIC-Electronic Privacy Information Center, http://epic.org/privacy/choicepoint/ (accessed April 13, 2011).

49 As a practical matter, standards for communicating contexts will be needed through interface design. See, for example, the work of Ryan Calo and Lorrie Cranor.

50 Nissenbaum, *Privacy in Context*, esp. chap. 8–9.

51 Danielle Citron, "Fulfilling Government 2.0's Promise with Robust Privacy Protections," *George Washington Law Review* 78 (4) (June 2010): 822–845.