Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't

Author(s): Daniel Susser

Source: *Journal of Information Policy*, Vol. 9 (2019), pp. 37-62

Published by: Penn State University Press

Stable URL: https://www.jstor.org/stable/10.5325/jinfopoli.9.2019.0037

Accessed: 04-03-2019 02:40 UTC

NOTICE AFTER NOTICE-AND-CONSENT

Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't

Daniel Susser

ABSTRACT

The dominant legal and regulatory approach to protecting information privacy is a form of mandated disclosure commonly known as "notice-and-consent." Many have criticized this approach, arguing that privacy decisions are too complicated, and privacy disclosures too convoluted, for individuals to make meaningful consent decisions about privacy choices—decisions that often require us to waive important rights. While I agree with these criticisms, I argue that they only meaningfully call into question the "consent" part of notice-and-consent, and that they say little about the value of notice. We ought to decouple notice from consent, and imagine notice serving other normative ends besides readying people to make informed consent decisions.

Keywords: information privacy, notice, consent, mandated disclosure, autonomy

The dominant legal and regulatory approach to protecting information privacy is a form of mandated disclosure commonly known as "notice-and-choice" or "notice-and-consent." Rather than directly regulating information practices, notice-and-consent simply requires that individuals be notified and grant their permission before information about them is collected and used. While there are a number of benefits to this approach—it's cheap, encourages innovation, and appeals to individual choice—it has come under sustained criticism. Philosophers and legal theorists argue that the cost of opting out of services is often too high to represent a meaningful choice for individuals to make. In cases where they might reasonably opt out individuals are frequently ill-equipped to fully understand the decision they face. And even when they do understand it, what is at issue

Daniel Susser: College of Information Sciences & Technology and Rock Ethics Institute, Penn State University

JOURNAL OF INFORMATION POLICY, Volume 9, 2019

in the decision is often a social rather than individual interest. In such cases individuals should not be deciding about it in the first place.

On account of these problems many of notice-and-consent's critics call for a move to more substantive regulation. They do not advocate abandoning notice-and-consent entirely, but urge us to recognize its limitations and count on it to do only as much work in upholding privacy norms as it is able. How much work that is exactly remains somewhat unclear, but we are left with the impression that it isn't a lot.

These arguments are largely persuasive. I agree that the notice-and-consent approach is mostly ineffectual and that in order to protect people's privacy, we need therefore to implement more substantive regulations. In this article, however, I argue that the earlier considerations successfully call into question only the "consent" part of notice-and-consent, and that there are independent reasons for valuing notice. This is important because critics of notice-and-consent seem to assume that consent is the crucial component, that notice is valuable only because (in theory) it makes informed consent possible. Thus, having shown that consent fails to further the normative aims we look to it for—to make data practices deferential to individual preferences and interests—they assume to have undermined the case for notice too.

I argue that we shouldn't throw the baby out with the bathwater. While critics of notice-and-consent are right that we ought to marginalize the role of individual consent in privacy regulation, that does not entail marginalizing the role of notice in equal proportion. To show that we ought to abandon the practice of mandated privacy disclosures, critics must evaluate notice on its own terms. While helping us decide whether or not to consent to specific data practices is one purpose notice could serve, it may also be valuable for other reasons. Indeed, the very arguments for moving away from consent-oriented regulatory approaches themselves counsel in favor of holding onto notice. If the problem with notice-and-consent as a whole is that it fails to facilitate and respect individual agency over data, then we ought not to deprive ourselves of even flawed and partial mechanisms for strengthening such agency. As I attempt to show, notice—shorn from consent procedures—can act as one such mechanism. This argument aligns with mounting demands by privacy advocates for increased transparency around data-driven systems.[1] Privacy disclosures are one of the few existing and established transparency tools we have.

1. Pangburn.

What's more, calls to abandon the notice-and-consent model arrive at a particularly inopportune moment. First, because our technologies and the sociotechnical systems they are embedded in are increasing in complexity, it is likely increasingly difficult for the average person to understand them and the stakes of using them. Users need more information about the data practices they are implicated, not less, now more than ever.[2] Second, the political climate—at least in the United States—bodes poorly for passing the kind of substantive privacy regulations notice-and-consent's critics envision.[3] It would be imprudent, at best, to sacrifice what tools we have for better tools we may never get.

With this in mind, I proceed as follows. In the first section, I review the arguments against notice-and-consent more closely, with an eye toward pinpointing the precise target of its critics' normative worries. Having found that the target is consent (and not notice), I pull the two apart, and I discuss why we ought to evaluate notice on its own terms. Finally, I attempt to place notice on firmer normative ground by offering some suggestions for why we ought to value notice in a world that has moved past the notice-and-consent framework.

The Rise and Fall of Notice-and-Consent

Privacy regulation in the United States is guided by the "Fair Information Practice Principles" (FIPPs), a set of recommendations originally developed by the U.S. Department of Health, Education, and Welfare (HEW) in 1973.[4] Recognizing the threat to individual privacy posed by the government's move toward computerized record-keeping, HEW Secretary Caspar Weinberger tasked a committee with articulating principles for safeguarding it. The committee defined privacy as "control by an individual

2. Of course, too much information can also be a problem. What is needed is information well-selected and well-presented. See Carr; and Andrejevic; and the section "Notice Unchained."

3. There is some reason for hope that this situation might be changing. Recently proposed federal legislation known as the "Data Care Act" would in fact guarantee some important substantive protections, and it demonstrates that many U.S. lawmakers are aware of these problems. However, the bill is not likely to pass. See Lecher. The situation is somewhat more promising at the state level. A number of states, including California, Vermont, and Colorado, have enacted state-level privacy protections, and a number of other states are considering following suit. However, most of these protections focus on strengthening existing consent-based frameworks rather than placing substantive limits on data practices. See Gilliland.

4. Gellman.

over the uses made of information about him," and it designed the FIPPs to bolster that control.[5] The report put forward five broad principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Since 1973, the FIPPs have been further developed and refined, and they have been put into practice in a variety of different ways. The Organization for Economic Cooperation and Development (OECD) used them as a model for developing European privacy guidelines in 1980.[6] The OECD rules were superseded in 2018 by the EU General Data Protection Regulation (GDPR), which retains the previous framework's emphasis on individual informed consent.[7] In Europe, privacy rules govern both public and private sector data collection.[8] In the United States, we have taken a more piecemeal approach. The Privacy Act of 1974 adopted the FIPPs directly, but applies only to information collected and stored by federal government agencies (5 U.S.C. § 552a). Other laws, like the Health Insurance Portability and Accountability Act (HIPAA) and the Fair Credit Reporting Act (FCRA), use versions of the FIPPs to regulate both public

5. U.S. Department of Health, Education, and Welfare. It is important to note that this understanding of privacy is not universally held. Philosophers, legal theorists, and privacy advocates have argued for alternative definitions of privacy, such as privacy as limited access, privacy as secrecy, and privacy as contextual integrity. Privacy understood as the ability of individuals to control information about themselves is, however, the operative definition at work in the vast majority of U.S. policy discussions. Therefore, despite its conceptual and practical shortcomings, it is the definition I assume for the sake of argument here. For a helpful discussion of various approaches, see Chapter 4 in Nissenbaum, *Privacy in Context*.

6. Gellman, 6–8.

7. European Union Agency for Fundamental Rights, European Court of Human Rights, and Council of Europe.

8. Cate, 350.

and private sector data collection, but only with respect to certain specific kinds of data.

When it comes to the vast majority of commercial data collection in the United States, privacy guidelines are, as Robert Gellman writes, "mostly voluntary and sporadic."[9] As there is no single, overarching data privacy law, the main way the government pushes private firms to comply with privacy principles is through the threat of Federal Trade Commission (FTC) enforcement actions. Businesses are encouraged to issue privacy policies, which describe—often in excruciating detail—what information they collect about their users and how they intend to use it. And through its authority to prosecute "unfair and deceptive" trade practices, the FTC then ensures that those businesses keep to their word.[10]

In 2000, the FTC issued a report outlining its own version of the FIPPs, which it offered as guidance for designing commercial privacy policies. Unlike the HEW report FIPPs, which included a mixture of substantive and procedural norms, the FTC's recommendations drop the substantive concerns about data reliability and purpose specificity and focus almost entirely on procedural guidelines for ensuring user control.[11] The FTC recommends that private businesses collecting user information offer

1. Notice—Websites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through nonobvious means such as cookies), how they use it, how they provide choice, access, and security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
2. Choice—Websites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).
3. Access—Websites would be required to offer consumers reasonable access to the information a website has collected about them,

9. Gellman, 20.
10. Cate, "The Failure of Fair Information," 352.
11. Ibid.

including a reasonable opportunity to review information and to correct inaccuracies or delete information.

4. Security—Websites would be required to take reasonable steps to protect the security of the information they collect from consumers.[12]

In other words, businesses can do what they want with user information, provided (1) they tell users that they are going to do it and (2) users choose to proceed.[13] This is the notice-and-consent model.

It's worth pausing for a moment to note that in the FTC framework (and related guidelines) notice (1) and consent (or "choice") (2) are offered as two independent principles. Notice ensures that users are aware of a firm's data practices; consent ensures that they are only implicated in those practices if they want to be. This is important, because, as we will see, critics of notice-and-consent tend to treat them as a single norm.

There are many things to like about the FTC's emphasis on procedural rather than substantive regulations. First, as both admirers and critics point out, notice-and-consent reflects a free-market approach to privacy: almost any behavior is permitted as long as all of the parties contractually agree to it.[14] The role of government, in this model, is merely to ensure that the contracts are enforced. From the perspective of businesses, this allows for a kind of flexibility that (it is claimed) is essential to commercial competitiveness.[15] The real value of user information is often discovered only after it's collected. Requiring companies to use information solely for purposes specified in advance could plausibly hamper their ability to innovate. Likewise, from the perspective of users, notice-and-consent is designed to be responsive to their preferences. Some users care more about who has information about them than others, and the notice-and-consent approach gives individuals the opportunity to express their desires and

12. U.S. Federal Trade Commission, 36–37. The FTC first issued privacy guidelines in 1998, which included notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. It updated its recommendations in 2000, dropping the "enforcement/redress" principle. See Gellman, 20–21. As Gellman notes, since 2000 the FTC has issued inconsistent guidelines regarding the FIPPs (Ibid., 21).

13. As in this footnote, access and security are, for the FTC, second in importance to notice-and-consent. As Reidenberg et al., write: "The FTC has identified notice as '[t]he most fundamental principle' in online privacy" (citing the FTC's 2000 Report).

14. As Solove writes, "Consent legitimizes nearly any form of collection, use, or disclosure of personal data" (1880). Also see Nissenbaum on "the compatibility of notice-and-consent with the paradigm of a competitive free market" ("A Contextual Approach," 34).

15. "Lawmakers and officials in the United States have refrained from heavy-handed restrictions on the flow of information out of a fear of stifling innovation—a fear shared by academics" (Calo, 1048).

interests. If they want to, it allows people to sell their personal information or to exchange it for services. While at the same time, it is meant (in theory) to protect those who would rather not have information collected about them from having it collected against their will.

Furthermore, from the FTC's perspective, notice-and-consent is easy to implement and cheap to enforce.[16] Rather than regulators having to determine which data practices are acceptable and which are not, in which contexts and under what circumstances, and to keep up with social and technological developments that might alter those determinations, the notice-and-consent approach allows the FTC simply to verify that commercial organizations are complying with the terms the organizations themselves specify. Instead of having to do the difficult normative work of deciding whether or not particular data practices are ethically and politically legitimate, regulators need only look to see if users have agreed to the terms of an organization's privacy policy. If they have, then the practices described in the policy are considered *prima facie* acceptable.

As an overarching regulatory scheme, notice-and-consent thus offers something for everyone. In theory, businesses, their customers, and the regulators overseeing them, all benefit in some way from an approach that restricts itself to procedural concerns. Nevertheless, notice-and-consent has come under sustained criticism. While good for businesses, notice-and-consent fails to deliver for consumers. Philosophers and legal theorists argue that for a variety of reasons it offers not choice, but merely the *illusion* of choice. It claims to be responsive to user preferences and interests, but in fact serves to obscure the actual conditions under which user information is collected, stored, transmitted, and used. If the normative core of notice-and-consent is its promise to give users control over information about themselves, critics of notice-and-consent argue that it fails to live up to that promise.

They level five main criticisms. First, they argue that notice-and-consent fails to offer real options for consumers to choose from. The decision is typically all-or-nothing: accept the terms and conditions set forth in the terms of service (TOS) or end-user license agreement (EULA) or do not engage with the product or service at all. And the latter is often not a realistic option, since the cost of opting out is often too high. If, for instance, the choice is between accepting a social network's privacy policy and getting to see pictures of one's grandchildren, or rejecting the policy's terms

16. Ben-Shahar and Schneider, "The Failure of Mandated Disclosure," 103.

and not getting to see them, many grandparents will not view the latter as an acceptable option. As Helen Nissenbaum puts it: "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."[17]

Second, critics argue that even when a company provides users with real options, they are often ill-equipped to understand and evaluate them. Most people do not read privacy notices.[18] Those who do are confronted with notoriously long, technical contracts rendered in dense legalese.[19] If the reader is trained to decode the legal jargon, they will still need a great deal of technical background knowledge to make sense of the content. Furthermore, as Solove argues, even if the average user could understand the average privacy policy they would face a variety of common decision-making problems.[20] Bounded rationality issues, such as availability heuristics and framing effects, make it exceedingly difficult for individuals to weigh the costs of particular data practices against their own privacy interests.[21] "The situation nearly approaches that faced by the protagonist in Franz Kafka's parable *Before the Law,*" Solove writes, "where the gateway was guarded by an infinite set of doorkeepers, each more powerful than the next."[22]

Importantly, the firms presenting users with these options do not face the same problem. Which is to say, significant information asymmetries exist between users and the organizations with which they are contracting. While—for the reasons described earlier—users will generally have difficulty evaluating the costs and benefits of particular data practices, firms will not. As Chris Hoofnagle and Jan Whittington write, "the firm is aware of its cost structure, technically savvy, often motivated by high-powered incentives of stock values, and adept at structuring the deal so that more financially valuable assets are procured from consumers than consumers would prefer."[23] This asymmetry introduces questions about the relative power of these different parties and whether the terms they reach are fair.[24]

17. Nissenbaum, "A Contextual Approach," 35.
18. Nissenbaum, *Privacy in Context*, 105. Citing Kandra and Brandt.
19. Ben-Shahar and Schneider, "The Failure of Mandated Disclosure."
20. Solove.
21. Hanna.
22. Solove.
23. Hoofnagle and Whittington, 640–41, quoted in Hull.
24. I am grateful to an anonymous reviewer for emphasizing this point.

The third problem is that notice-and-consent simply does not scale. Most of us engage with a huge number of information actors—commercial websites and apps, government agencies, educational institutions, and so on. While we might be expected to read, understand, and evaluate a few of their privacy policies, it is inconceivable that we could keep up with them all.[25] Furthermore, as Nissenbaum points out, the arrangement of information actors working behind the scenes is a "shifting landscape." The entity directly collecting information about us might store it on servers elsewhere, pass it along to others for further processing, or sell it. "The technical and institutional story is so complicated," Nissenbaum argues, "that probably only a handful of deep experts would be able to piece together a full account [. . .] 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."[26]

If the huge number of information actors we deal with is a problem, then the huge amount of information itself is an even bigger one. The fourth criticism of notice-and-consent is what Solove describes as "the problem of aggregation." Things about us which do not seem particularly sensitive can, in the aggregate, reveal deeply personal information. Which is to say, the sum of data about us is greater than its parts. When individuals weigh the costs and benefits of disclosing particular pieces of information, they can't know what other information it will be combined with down the road. Notice-and-consent thus demands that we make onetime decisions that can have cascading effects, and we are in principle unable to predict those effects at the moment of decision.[27]

Fifth and finally, critics of notice-and-consent point out that the interests privacy protects are not only individual interests, but social or collective interests too. Priscilla Regan and Joel Reidenberg both argue, for instance, that privacy has social benefits.[28] Julie Cohen argues that privacy is necessary for individual creativity and innovation, which in turn are

25. In 2008, McDonald and Cranor estimated that it would take the average person 244 hours per year (or 40 minutes per day) to read all the relevant privacy policies they encountered online. That estimate does not gauge how long it would take to *comprehend* the policies—just to read the texts. Mcdonald and Cranor, 26.

26. Nissenbaum, "A Contextual Approach," 35. See also Barocas and Nissenbaum, 7.

27. For a helpful discussion of this problem see Nissenbaum, "Toward an Approach to Privacy in Public."

28. Regan; Reidenberg.

necessary for ethical and cultural development.[29] Lior Strahilevitz draws attention to the distributive effects of different privacy regimes.[30] And for Nissenbaum, privacy is—in the first place—a set of social norms, not a set of individual decisions. Privacy norms "preserve the integrity of the social contexts in which we live our lives, and they support and promote the ends, purposes, and values around which these contexts are oriented."[31] On the notice-and-consent model of privacy regulation individuals are made to decide about the fate of social goods.

To summarize, then, the main arguments against notice-and-consent are

1. It offers only all-or-nothing decisions, and the cost of opting out is often too high to represent a meaningful choice.
2. Privacy policies are too difficult to understand, and widespread cognitive problems make individuals bad at weighing the costs and benefits of particular data practices.
3. Notice-and-consent doesn't scale—there are too many information actors to keep up with, and they constitute a constantly shifting landscape.
4. Data aggregation makes it difficult, if not impossible, to know in advance how revealing particular pieces of information are.
5. Privacy protects both individual and social interests, and individuals ought not to be in the position of deciding whether or not to safeguard social goods.

Arguments 2–4 can be described together in broader terms: individuals are ill-equipped to make the kinds of decisions notice-and-consent requires them to make. So the five criticisms earlier can really be described as three:

1. Notice-and-consent fails to offer real choices.
2–4. What choices it offers we are ill-equipped to make.
5. It asks us to make choices that shouldn't be ours to make.

For these reasons, privacy scholars argue that we ought to move away from strictly procedural privacy regulations and toward more substantive controls. Nissenbaum and Solon Barocas "support substantive direct regulation."[32] Solove calls for "more substantive rules about data collection, use,

29. Cohen.
30. Strahilevitz, 33.
31. Nissenbaum, *Privacy in Context*, 186.
32. Barocas and Nissenbaum.

and disclosure," with "hard boundaries that block particularly troublesome practices as well as softer default rules that can be bargained around."[33] Joel Reidenberg and his colleagues at the Fordham Center on Law and Information Policy suggest that notice-and-consent is effective at protecting against *some* privacy-related harms (unauthorized disclosures, surreptitious collection), but not others (data security, wrongful retention), and regulators ought to rely on it to do only as much work as it's able.[34] None of these critics argues that notice-and-consent ought to be abandoned *entirely*, but their arguments suggest that it does not have a significant role to play in any truly privacy-protective future.[35]

I find these arguments persuasive. Notice-and-consent appears to be a failed regulatory model. Normatively, it was designed to give users control over information about themselves, but it manages only the semblance of control. For all of the reasons described earlier, when users agree to the terms of commercial privacy policies, there is little reason to believe they are expressing real preferences. Their consent reflects resignation not deliberation. Assuming, then, that *consent* has failed, and it ought to be abandoned, should notice be abandoned too?

Decoupling Notice and Consent

Implicit in the critiques discussed earlier is a theory of the relationship between notice and consent. On this theory, consent is the normatively salient term. It is the mark, the imprimatur, of respect for individual preferences. If notice-and-consent offers a procedural form of privacy, then consent is—both literally and figuratively—the end of the procedure.

Notice, on the other hand, is simply a means to that end. In order for consent to be meaningful, it must be *informed*. To treat the signature at the end of a privacy policy (or the "I Agree" clicked at the bottom of a screen) as a real testament of the user's will, we have to assume that the user understood the decision being made. Were they ignorant or deceived their consent might not reflect their true preferences. The point of notice is to facilitate that understanding; it's meant to provide the information

33. Solove, 1903.

34. Reidenberg et al., 29.

35. For additional recommendations that we move away from purely procedural privacy regulations and toward more substantive controls, see Cate.

users need to make free, reasoned decisions. As Omri Ben-Shahar and Carl Schneider write: "mandated disclosure [i.e., notice] addresses the problem of a world in which nonspecialists must make choices requiring specialist knowledge. Its solution is alluringly simple: if people face unfamiliar and complex decisions, give them information until the decision is familiar and comprehensible."[36]

The arguments discussed in the previous section demonstrate that privacy disclosures fail to fulfill this function. They are too difficult to understand. There are too many to keep up with. They describe only the near-term effects of disclosing information about ourselves; what that information will reveal once aggregated is unknowable in advance. As such, the consent offered when individuals sign privacy policies, click through clickwrap agreements, or agree to long, unreadable TOS contracts, is not meaningful consent. It does not represent careful, deliberate, and informed decision-making, but rather a pro forma gesture. And such gestures cannot legitimate the collection and use of user information.

Understood in this context, the rationale for throwing out notice along with consent is as follows: What we care about is consent. In order for consent to legitimate certain behaviors and practices, the consenter must have a certain threshold level of knowledge or understanding about the decision he or she faces. Notice is meant to help provide that understanding, but it fails to do so. Consequently, consent fails to do the work we need it to do. Absent consent, there is no job for notice. Or to put it another way, critics of notice-and-consent assume that consent is the crucial bit, and notice is valuable only because (in theory) it makes informed consent possible. Thus, having shown that consent fails to further the normative aims we look to it for—to make policy deferential to individual preferences and interests—they assume to have undermined the case for notice too.

But what if notice fulfills—or could fulfill—other functions? That it fails to provide the level of understanding required to make informed consent decisions does not mean it fails to provide any understanding at all. Indeed, the degree of understanding required for informed consent is extremely high. When we make informed consent decisions, we usually waive some of our rights. (Notice-and-consent might more accurately be called "notice-and-waiver," its point being less to give users meaningful agency in navigating the informational landscape and more to shield the government and private firms from liability around their data practices.)

36. Ben-Shahar and Schneider, *More Than You Wanted to Know*, 5.

We take on the entire burden of responsibility for the outcomes of the set of actions we consent to. In order to offer that kind of consent, we need to have a deep and complex picture of the choice we are making.[37] Yet for lots of other important things we might do or want to do, a lesser degree of understanding might suffice. To say that notice doesn't provide enough meaningful information to meet the very highest bar is not to say the information it does provide isn't valuable at all.

One reason this possibility has not been given due consideration likely stems from the particular conception of the subject that proponents of notice-and-choice imagine to be its beneficiary. As Julie Cohen argues that conception is inherited from traditional liberal political theory and understands subjects as "rational choosers."[38] These are the idealized protagonists of rational choice theory, who decide how to act by gathering information and using it to evaluate the expected utility of their options. Cohen describes the rational chooser as a "definitionally autonomous being who experiences unbroken continuity between preference and action."[39] Since the chief normative commitment that liberal political theory aims to realize is respect for individual preferences, and since the rational chooser is understood as being able to signal their preferences unproblematically via consent decisions, operationalizing liberal theory's normative commitment appears to be fairly straightforward: just ask individuals whether or not they consent to different forms of treatment. In the case of information privacy, this means asking them whether or not they consent to particular information practices.

Given these background assumptions, it is no wonder that the value of the notice-and-consent regime has traditionally been understood to revolve around the consent part. If user consent decisions are not worth anything, surely the disclosures meant to prepare users to make them

37. The idea of informed consent was originally developed in the field of bioethics. Describing its demands, bioethicist Beauchamp writes that informed consent is legitimate "if and only if the person, with *substantial understanding* and in substantial absence of control by others, intentionally authorizes a health professional to do something" (517–18, emphasis mine).

38. Cohen, 110–15. In fact, Cohen argues that American privacy law is disjointed, imagining two incompatible beneficiaries of its protections. Constitutional law, on the one hand, understands the subject as a "romantic dissenter" who values privacy because it protects their ability to dissent from prevailing public opinion and express unpopular views. Information privacy law, on the other hand, is the domain of the "rational chooser," who treats privacy as only instrumentally valuable, and therefore something one can (and should) trade for other goods. The notice-and-consent framework is a product of the latter.

39. Ibid., 112

are not worth anything either. As Cohen and many others have argued, however, the liberal conception of the subject and its attendant notion of autonomy are not the only game in town.[40] A deeper account, which truly reflected respect for persons (and their ability to choose), would acknowledge that we are imperfect decision-makers, bounded by a variety of limitations. While it is true that under such imperfect conditions, the kind of consent decision notice-and-consent asks users to make is little more than lip service (and legal cover for the data holder), providing users with disclosure information anyway can strengthen their decisions, even though they remain imperfect ones.

Indeed, one of the most prominent (and liberal) accounts of autonomy—that offered by Joseph Raz—understands autonomous decision-makers in just this way. As Raz writes, "The autonomous person is a (part) author of his own life. The ideal of autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives."[41] For Raz, we are *part* authors of our own lives, rather than full authors, because we are shaped by a variety of forces, from the nature of our upbringings to the social contexts in which we make important life decisions. Nevertheless, we are able to act autonomously because we are able, more or less, to "make [our] own lives."[42] That means having an adequate variety of options and being free from coercion or manipulation when choosing from amongst them, but it does not require having perfect information about the choices we confront. "To choose one must be aware of one's options," Raz argues, "[. . . One] must be capable of understanding how various choices will have considerable and lasting impact on his life."[43] Legalistic attempts to solicit an individual's consent are not, on this account, demonstrations of respect for individual autonomy. To respect autonomy, understood in this way, one would attempt to help people understand their options, as best they can, so that they can identify with and endorse their choices once they are made. In the next section, I offer some examples of how disclosures can do this important-if-imperfect work.

Before moving on, it is also worth pointing out that calls to move away from notice-and-consent come at a particularly inopportune moment—a

40. See, for example, Christman; Mackenzie and Stoljar.

41. Raz, 369.

42. Ibid.

43. Ibid., 371.

moment in which the average person's awareness of how they are implicated in everyday data practices is likely decreasing.[44] The trend in technology development is toward streamlining the user experience such that none of the underlying hardware and software processes are visible to the user.[45] In terms of user experience that is probably to the good, but when it comes to privacy, it isn't. It means that people will continue to have little idea about what information is being collected about them, by whom, or for what purposes.[46] And this will be happening at the same time as the amount of data collected about them, and the number of parties collecting it, continues to grow.

Calls to sideline notice-and-consent thus come precisely when we need notice most. While it's clear that we cannot rely on it to provide the level of understanding required for individuals to take on the full burden of responsibility for evaluating commercial data practices, it might help keep us from being cast totally into the dark. Quasi-informed citizen-consumers are preferable to mostly ignorant ones. What's more, if notice and consent are no longer paired, if consent is no longer the normative end to which notice aspires, then perhaps notice can take new forms. Perhaps we could simplify notice, or make it more "visceral." Arguments against this kind of simplification have traditionally assumed that the goal is consumer consent. Having shifted notice's purpose, such arguments lose their force.[47]

I propose, then, that we relax the standards placed on notice and see if it might do any good for us. Let us imagine that we have followed the advice of notice's critics and moved toward more substantive regulation, and let us see if there are roles for notice to play still.

---

44. Acquisti, Brandimarte, and Loewenstein argue, for example, that "Advancements in information technology have made the collection and usage of personal data often invisible. As a result, individuals rarely have clear knowledge of what information other people, firms, and governments have about them or how that information is used and with what consequences."

45. See Norman.

46. Cohen calls this a lack of "operational transparency" (234–39).

47. In their "definitive work" on the failures of mandated disclosure regimes, for instance, Ben-Shahar and Schneider write, "Whether mandated disclosure works depends on its goals," and they canvas existing regulatory structures to demonstrate, forcefully, that its goal—in U.S. law—has always been to equip consumers to make informed decisions (*More than You Wanted to Know*, 34.) When they argue against simplification (Chapter 8), this remains the background assumption. They do not entertain the possibility that the goal of mandated disclosure regulation could be changed.

The Virtues of Notice

Imagine we have done what notice-and-consent's critics would have us do (and I agree we should do). We put in place a set of substantive privacy regulations—"hard boundaries that block particularly troublesome practices as well as softer default rules that can be bargained around," as Solove suggests.[48] As with food safety regulations, these "hard boundaries" around data practices would protect us from clear, obvious harms. They would allow us to operate on the assumption that the information actors we transact with cannot simply do anything they want with the sensitive information about us they collect—an assumption we cannot operate on at present. With such protections in place individuals would be reasonably assured that making data about themselves available to organizations and private firms is fundamentally safe, even without any vigilance on their part. Beyond that protective floor, however, there would remain a vast realm of data practices about which people would continue to disagree.

The question then is: what work could notice do in this world? What value is there in mandated privacy disclosures once minimal substantive regulations are in place? In what remains, I discuss a number of plausible answers to these questions, which I group broadly into two categories: notice's *direct* and *indirect* benefits. First, I describe roles notice could play directly in support of user decision-making at the individual level, by making individuals aware of salient features of the informational landscape. Second, I point to the work notice can do to support users *indirectly*, either by empowering other parties who advocate for users, or by encouraging those who build data-driven tools to do so with user interests in mind. Importantly, this is not intended as an exhaustive list. It is simply a starting point, a proof-of-concept that will hopefully serve as motivation to think more actively about the positive work notice can do in a world after notice-and-consent.

The Direct Benefits of Notice

As I argued in the previous section, critics of notice-and-consent are right to charge that privacy disclosures are insufficient instruments for providing individual users with a deep enough understanding of the informational practices they are implicated in to facilitate consent decisions related to

48. Solove, 1903.

those practices that meaningfully reflect user choice. Having taken consent out of the picture, however, and having thus lowered the epistemic bar for the kind of understanding we expect notice to enable, we are now in a position to constructively ask what of value users might learn from privacy notices.

One purpose notice could serve is providing basic situational awareness. Lost amidst the "complex and shifting landscape" of information actors that Nissenbaum warns us about, it is difficult for the average end user (indeed, it is difficult even for the expert) to figure out who is collecting information about them, when, and for what purposes.[49] Even if substantive privacy regulations assured us that interacting with these information actors was safe, we still might want to know who has information about us and what they are doing with it. As we've seen, privacy disclosures rarely provide sufficient understanding to enable individual control over those actors, but notices might nevertheless meet a lower bar. Websites or apps could warn users if the information they collect will be sent to a third party for processing, if it will be aggregated with other user information, or if it will be sold.

That information could, in turn, help individuals flag prima facie privacy problems. For example, most of the time it wouldn't surprise us to learn that the websites we use transmit information about us to third parties for processing. If we learned, though, that a cloud storage service like Dropbox or Google Drive did that it might give us pause. Since many people store sensitive documents in cloud storage, they might want to know where exactly those documents were being sent, for what purposes, what security measures protected them, and what legal obligations those third parties owed them. We are better equipped to spot potential issues if we're armed with even *some* information about the data practices implicating us. And once we are aware of such issues, we can press for more information, enlist the help of experts (discussed further in the following), and so on.

Second, notice can equip us with the information needed to protect our privacy through *nonlegal* means. This is related to the idea of providing situational awareness, but is more directed. For some people, knowing that basic substantive privacy protections are in place will be enough to put to rest all their privacy worries. If they don't place a high personal premium on their privacy, then knowing that minimal safeguards exist to protect

49. Nissenbaum, "A Contextual Approach," 36.

them from plainly harmful practices could be all the peace of mind they need. But other people will want more. Political dissidents or activists, or people who work with sensitive trade secrets, for example, might want a higher level of privacy around their personal information than regulation will provide.

In order to secure that added privacy, privacy-demanding users might look beyond the law. They could choose to withhold certain information. They could look to engineering solutions, such as "privacy-enhancing technologies" (PETs).[50] Or, as Nissenbaum and Finn Brunton suggest, they could engage in *obfuscation*—"the production of misleading, ambiguous and plausible but confusing information as an act of concealment or evasion."[51] For Nissenbaum and Brunton, obfuscation is a toolkit for protecting one's privacy that individuals can look to precisely when they have reason to believe legal protections are insufficient. It is "an alternative strategy of informational self-defense, a method that acts as informational resistance, disobedience, protest or even covert sabotage."[52] Yet in order to engage in any of these forms of self-directed, extralegal, privacy-protective behaviors, individuals need to have at least a rough sense of the informational landscape they're operating in. Engaging in effective obfuscation, for example, requires knowing when and where and what to obscure. While notice can't provide the level of awareness informed consent demands, it could facilitate a level of awareness that is useful for achieving these other goals.

Third, notice can alert us to the fact that we need to assert other rights. Recent discussions about digital due process rights, for instance, demand that individuals know when they are in a situation in which those rights should be exercised. Danielle Citron argues that one way the automation of administrative decision-making processes—such as when to terminate Medicaid or other welfare benefits—deprives people of due process is that it deprives them of notice that decisions are being made about them, and of rationales explaining how they arrive at the decisions they do.[53] This problem is only exacerbated by Big Data. Building on Citron's work, Kate Crawford and Jason Schultz argue that we ought to require "those who use Big Data to 'adjudicate' others—i.e., those who make categorical or

50. For an overview of such approaches, see Gürses and del Alamo.

51. Brunton and Nissenbaum, "Political and Ethical Perspectives," 164.

52. Ibid.; see also Brunton and Nissenbaum, *Obfuscation*.

53. Citron, 1305.

attributive determinations—to post some form of notice, disclosing not only the type of predictions they attempt, but also the general sources of data that they draw upon as inputs, including a means whereby those whose personal data is included can learn of that fact."[54]

The Indirect Benefits of Notice

In addition to directly raising user awareness in the ways described earlier, notice can play an indirect role in supporting user interests. Notice can empower third parties that advocate on behalf of users, and the process of creating privacy notices can serve as a prompt to firms building data-driven technologies to reflect on and improve user privacy.

Thus far in this discussion, I have implicitly understood individual end users to be the primary audience for privacy disclosures. When notice is attached to consent procedures, that assumption is warranted, since it is individual end users whose consent is being solicited. If notice was decoupled from consent, however, the audience could change. Beyond raising individual user awareness about the data practices implicating them (in admittedly imperfect, epistemically nonideal ways), notice could provide valuable information to regulators or to third parties that advocate for users' interests. There are a large number of nongovernmental and other civil society organizations that work to strengthen privacy protections in a variety of ways—from educating individuals and litigating on their behalf to crafting and promoting policy.[55] Such organizations, staffed by lawyers, technologists, and privacy experts, are not bound by the same limitations as individuals confronting long, technical disclosures rendered in opaque legalese. With individual consent no longer the motivation behind and purpose for disclosures, we could imagine their value being mediated through third-party privacy advocates. What's more, such organizations are better positioned to help realize privacy's social—in addition to its individual—importance.[56] Organizations such as the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC) spend considerable time and effort filing Freedom of Information Act requests to force government agencies to disclose information about data

54. Crawford and Schultz, 125.

55. See Bennett.

56. See section, "The Rise and Fall of Notice-and-Consent."

collection and other surveillance practices.[57] Absent mandated disclosure requirements, there are few comparable avenues for gaining access to information about the practices of private firms.[58]

Furthermore, notice can encourage good corporate behavior. Which is to say, beyond the value of the information itself (either to individuals or third parties), there is reason to believe that simply forcing companies to express what they intend to do with user information—whether publicly or internally to their own organization—can help induce them to come into compliance with social norms. A case study of this effect can be found in Peter Swire's analysis of corporate responses to the financial privacy regulations introduced by the 1999 Graham–Leach–Bliley (GLB) Act. One requirement of the law is that financial organizations are required to provide consumers with annual disclosures about their privacy policies. Despite the fact that—like the privacy notices discussed earlier—GLB notices are usually rendered in dense, complex legalese, Swire found that "in order to draft the notice, many financial institutions undertook an extensive process, often for the first time, to learn just how data is and is not shared between different parts of the organization and with third parties."[59] And he concluded that "many institutions discovered practices that they decided, upon deliberation, to change."[60] Similarly, Paula Bruening and Mary Culnan argue that "While not originally envisioned to function in this way, the drafting of a privacy notice provides a company with an opportunity to inventory and assess internal practices, making sure they are up to date, necessary, and appropriate. It can also serve as a platform for decision-making about whether to continue with a data practice or deployment of technology in light of considerations related to brand, and developments in law, policy, or market practices."[61]

Notice Unchained

While it's true, then, that privacy disclosures can't facilitate the level of understanding required for informed consent, the level of understanding

57. See https://www.eff.org/issues/transparency/foia-requests and https://www.epic.org/foia/.

58. Describing financial disclosures, Admati and Pfleiderer write: "Full voluntary disclosure, however, rarely seems to occur in reality, and firms typically do not disclose more than regulation requires," 480.

59. Swire, 1316 cited in Solove, fn. 85.

60. Ibid.

61. Bruening and Culnan, 542.

they *can* facilitate is still valuable for other reasons. There is plenty of work for notice to do in a world after notice-and-consent.

What's more, given these new purposes or ends toward which notice might be oriented, we should wonder whether it still needs to take on the form of the long, legal contract. After all, notice took that form in the first place in order to meet the high informational demands required for informed consent. As we've seen, consent decisions require deep and robust knowledge of what is at stake; the only way to facilitate that kind of understanding—to ensure that users could, in principle, consider the question from every angle—is to be *exhaustive.* Firms (or more precisely, their lawyers) therefore go to literal great lengths to describe every eventuality that might befall one's data. The threat of liability means companies cannot afford to hold anything back.

But if informed consent is no longer the goal, if deep, robust understanding is no longer the epistemological standard to which privacy disclosures are held, and if commercial firms are no longer legally responsible for facilitating that level of user understanding, maybe privacy policies won't need to be so exhaustive. Perhaps we could develop new "visceral" forms of notice, as Ryan Calo has suggested, and leverage auditory and other user experience cues to enhance user awareness, rather than rely solely on written disclosures.[62] Or perhaps notices could be standardized and simplified on the model of food nutrition labels.[63] Or we could require companies to disclose that they have significantly changed their privacy commitments by somehow altering their visible brand.[64] Schaub et al. point to a variety of considerations that ought to be taken into account when deciding how to structure an effective privacy disclosure, ranging from the timing of the notice to its audience and modality.[65]

In general, firms could start paying attention to both the content of their privacy policies and the *design* of the notices that convey them. As Ari Ezra Waldman argues, we are embodied decision-makers who rely on a wide range of visual and organizational cues in order to process and interpret information, and design choices therefore deeply influence our capacity to understand documents like privacy policies. In order to ensure that such policies are constructed in a way that users can

62. Ibid.
63. Ciocchetti; Cranor.
64. Ohm.
65. Schaub, Balebako, and Cranor.

actually comprehend them, Waldman suggests that disclosure designs be empirically tested before being implemented.[66] Skepticism toward efforts such as these—to reengineer disclosures in a way that makes them more useful to decision-makers—is usually rooted in the assumption that the sole purpose of notice is to furnish the information necessary to make informed consent decisions.[67] Were notice to be decoupled from consent and made to serve other purposes, such skepticism would lack warrant. If facilitating consent is no longer the *function* of notice, we can imagine its *form* changing too.[68]

Conclusion

Finally, two caveats. Privacy disclosures aren't without a downside. As Chris Hoofnagle and Jennifer King have pointed out, some users misinterpret the sheer presence of privacy policies as an indication that the websites or apps displaying them adhere to privacy-protective standards.[69] It is easy to imagine commercial firms leveraging this misunderstanding for their own gain. One reason why privacy advocates have worked to marginalize the role of notice-and-consent in the overall scheme of privacy regulation is that it requires users to shoulder more responsibility for vetting the data practices they encounter than they reasonably ought to shoulder. By trying to bring disclosure back into the picture I thus risk inadvertently giving already powerful actors—corporations, and other private and public organizations and institutions—normative cover.

If we are careful, though, these legitimate worries can be avoided. Spared from having to be exhaustive, privacy notices could be designed to truly facilitate user understanding, rather than to shield information actors from legal liability. If they are successful, users will be less likely to

66. Waldman.

67. See, for example, Ben-Shahar and Schneider, *More Than You Wanted to Know*, Part III.

68. Of course, this raises the question of how to define the legal standards by which these new forms of disclosure would be judged. Answering that question is outside the scope of this article, but it is worth emphasizing here that even though I have described a number of different roles notice could play in a world after notice-and-consent, I do not mean to suggest that its role or roles should remain undefined. My goal has been to demonstrate that notice could have value beyond informing individuals to make consent decisions. If my argument is persuasive, then we ought to carefully specify the work we want notices to do, and we ought to craft legal standards that ensure they can do it.

69. Hoofnagle and King.

misinterpret their meaning. Likewise, once consent (or waiver) has been replaced, at least in certain contexts, with substantive regulation, legitimating data practices will require evaluating the real risks and potential harms those practices carry, rather than simply evaluating compliance with written notices. Helping raise user awareness about the data practices they are implicated in should not relieve information actors of responsibility for not harming their users.

Critics of purely procedural privacy regulations are right to argue that notice-and-consent has failed to live up to its normative promises. Meaningful consent decisions require an extremely high level of awareness and understanding, and privacy disclosures cannot provide it. That users agree to the terms of commercial privacy policies is therefore poor evidence that those decisions reflect users' true preferences and interests. We should do as notice-and-consent critics suggest and institute substantive privacy regulations.

We move too quickly, however, when we infer from those arguments that notice and consent ought to be marginalized in equal proportion. Notice is a means, a regulatory instrument, and consent is but one possible end it might serve. Even in a world where we are protected by some number of substantive privacy regulations, there is plenty of work for notice to do. Though it cannot provide the level of understanding required to make informed consent decisions, it can provide a lesser level of understanding that meaningfully strengthens user decision-making in other ways.

It is especially important that we recognize this now. Calls to move past privacy disclosures come at the same time as end users are implicated in an increasingly vast universe of information practices, which—without mandated disclosure—they will have less and less information about. Thus, while debates about the value of consent for legitimating data practices will no doubt continue, we would do well to recognize that the value of notice is not contingent upon their answer.

BIBLIOGRAPHY

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. "Privacy and Human Behavior in the Age of Information." *Science* 347, no. 6221 (January 30, 2015): 509–14. doi:10.1126/science.aaa1465.

Admati, Anat R., and Paul Pfleiderer. "Forcing Firms to Talk: Financial Disclosure Regulation and Externalities." *The Review of Financial Studies* 13, no. 3 (2000): 41.

Andrejevic, Mark. *Infoglut: How Too Much Information Is Changing the Way We Think and Know*. New York: Routledge, 2013.

Barocas, Solon, 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*, 7, Massachusetts Institute of Technology, Cambridge, MA, October 2009.

Beauchamp, Tom L. "Informed Consent: Its History, Meaning, and Present Challenges." *Cambridge Quarterly of Healthcare Ethics* 20, no. 04 (October 2011): 515–23. doi:10.1017/S0963180111000259.

Bennett, Colin. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press, 2008.

Ben-Shahar, Omri, and Carl E. Schneider. *More Than You Wanted to Know: The Failure of Mandated Disclosure*. Princeton, NJ: Princeton University Press, 2014.

———. "The Failure of Mandated Disclosure." *University of Pennsylvania Law Review* 159 (2011): 103.

Bruening, Paula J., and Mary J. Culnan. "Through a Glass Darkly: From Privacy Notices to Effective Transparency." *North Carolina Journal of Law and Technology* 17, no. 4 (May 2016): 66.

Brunton, Finn, and Helen Nissenbaum. "Political and Ethical Perspectives on Data Obfuscation." In *Privacy, Due Process and the Computational Turn*, edited by Mireille Hildebrandt and Katje de Vries, 25. New York: Routledge, 2013.

———. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press, 2015.

Calo, M. Ryan. "Against Notice Skepticism in Privacy (and Elsewhere)." *Notre Dame Law Review* 87, no. 3 (2012): 47.

Carr, Nicholas G. *The Shallows: What the Internet Is Doing to Our Brains*. Norton pbk. [ed.]. New York: W.W. Norton, 2011.

Cate, Fred H. "The Failure of Fair Information Practice Principles." In *Consumer Protection in the Age of the Information Economy*, edited by Jane Winn K., 37. New York: Routledge, 2006.

Christman, John Philip. *The Politics of Persons: Individual Autonomy and Socio-Historical Selves*. Cambridge ; New York: Cambridge University Press, 2009.

Ciocchetti, Corey A. "The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices." *The John Marshall Journal of Information Technology & Privacy Law* 26, no. 1 (2008): 47.

Citron, Danielle Keats. "Technological Due Process." *Washington University Law Review* 85, no. 6 (2008): 66.

Cohen, Julie E. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven, CT: Yale University Press, 2012.

Cranor, Lorrie Faith. "Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice." *Journal on Telecommunications and High Technology Law* 10, no. 2 (2012): 36.

Crawford, Kate, and Jason Schultz. "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms." *Boston College Law Review* 55, no. 1 (2014): 37.

European Union Agency for Fundamental Rights, European Court of Human Rights, and Council of Europe. *Handbook on European Data Protection Law*. 2018 edition. Handbook/FRA, European Union Agency for Fundamental Rights. Luxembourg: Publications Office of the European Union, 2018.

Gellman, Robert. "Fair Information Practices: A Basic History." *SSRN Electronic Journal*, 2017. doi:10.2139/ssrn.2415020.

Gilliland, Donald. "States Are Leading the Way on Data Privacy." *The Hill*, August 21, 2018. https://thehill.com/opinion/technology/402775-states-are-leading-the-way-on-data-privacy.

Gürses, Seda, and Jose M. del Alamo. "Privacy Engineering: Shaping an Emerging Field of Research and Practice." *IEEE Security Privacy* 14, no. 2 (March 2016): 40–46. doi:10.1109/MSP.2016.37.

Hanna, Jason. "Consent and the Problem of Framing Effects." *Ethical Theory and Moral Practice* 14, no. 5 (2011): 517–31.

Hoofnagle, Chris Jay, and Jennifer King. "What Californians Understand about Privacy Online." *SSRN Electronic Journal*, 2008. doi:10.2139/ssrn.1262130.

Hoofnagle, Chris Jay, and Jan Whittington. "Free: Accounting for the Costs of the Internet's Most Popular Price." *UCLA Law Review* 61 (2014): 67.

Hull, Gordon. "Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data." *Ethics and Information Technology* 17, no. 2 (June 2015): 89–101. doi:10.1007/s10676-015-9363-z.

Kandra, Anne, and Andrew Brandt. "Great American Privacy Makeover." *PC World*, October 8, 2003. https://www.pcworld.com/article/112468/article.html.

Lecher, Colin. "Democratic Senators Have Introduced a Big New Data Privacy Plan." *The Verge*, December 12, 2018. https://www.theverge.com/2018/12/12/18138131/democratic-data-care-act-senate-law.

Mackenzie, Catriona, and Natalie Stoljar, eds. *Relational Autonomy: Feminist Perspectives on Automony, Agency, and the Social Self*. New York: Oxford University Press, 2000.

Mcdonald, Aleecia M., and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4, no. 3 (2008): 26.

Nissenbaum, Helen. "A Contextual Approach to Privacy Online." *Daedalus* 140, no. 4 (September 29, 2011): 32–48. doi:10.1162/DAED_a_00113.

———. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books, 2010.

———. "Toward an Approach to Privacy in Public: Challenges of Information Technology." *Ethics & Behavior* 7, no. 3 (September 1997): 207–19. doi:10.1207/s15327019eb0703_3.

Norman, Donald. *The Invisible Computer: Why Good Products Can Fail, the Personal Computer Is So Complex, and Information Appliances Are the Solution*. Cambridge, MA: MIT Press, 1999.

Ohm, Paul. "Branding Privacy." *Minnesota Law Review* 97 (2013): 907–89.

Pangburn, DJ. "How to Lift the Veil Off Hidden Algorithms." *Fast Company,* January 28, 2019. https://www.fastcompany.com/90292210/transparency-government-software-algorithms

Raz, Joseph. *The Morality of Freedom*. Reprinted. Oxford: Clarendon Press, 1986.

Regan, Priscilla M. *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill, NC: The University of North Carolina Press, 2009.

Reidenberg, Joel R. "Privacy Wrongs in Search of Remedies." *Hastings Law Journal* 57 (2003): 877–98. doi:10.2139/ssrn.434585.

Reidenberg, Joel R., N. Cameron Russell, Alexander Callen, Sophia Qasir, and Thomas Norton. "Privacy Harms and the Effectiveness of the Notice and Choice Framework," Paper presented at the 42nd Research Conference on Communication, Information and Internet Policy (TPRC), George Mason University School of Law, Arlington, VA, September 2014. doi:10.2139/ssrn.2418247.

Schaub, Florian, Rebecca Balebako, and Lorrie Faith Cranor. "Designing Effective Privacy Notices and Controls." *IEEE Internet Computing*, June 16, 2017, 1–1. doi:10.1109/MIC.2017.265102930.

Solove, Daniel J. "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126 (2013): 1880–903.

Strahilevitz, Lior Jacob. "Toward a Positive Theory of Privacy Law." *Harvard Law Review* 125 (2013): 33.

Swire, Peter P. "The Surprising Virtues of the New Financial Privacy Law." *Minnesota Law Review* 86, no. 6 (2002): 1263–324. doi:10.2139/ssrn.347402.

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." 1973. https://epic.org/privacy/hew1973report/default.html.

U.S. Federal Trade Commission. "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress." May 2000.

Waldman, Ari Ezra. "Privacy, Notice, and Design." *Stanford Technology Law Review* 21, no. 1 (2018): 129–84. doi:10.2139/ssrn.2780305.