2014

Beyond Notice and Choice: Privacy, Norms, and Consent

Richard Warner
Robert Sloan

Beyond Notice and Choice: Privacy, Norms, and Consent

Robert H. Sloan* and Richard Warner**

Abstract

Informational privacy is the ability to determine for yourself when and how others may collect and use your information. Adequate informational privacy requires a sufficiently broad ability to give or withhold free and informed consent to proposed uses.

Notice and Choice (sometimes also called "notice and consent") is the current paradigm for consent online. The Notice is a presentation of terms, typically in a privacy policy or terms of use agreement. The Choice is an action signifying acceptance of the terms, typically clicking on an "I agree" button, or simply using the website. Recent reports by the Federal Trade Commission explicitly endorse the Notice and Choice approach (and provide guidelines for its implementation). When the Notice contains information about data collection and use, the argument for Notice and Choice rests on two claims. First: a *fully adequate* implementation of the paradigm would ensure that website visitors can give free and informed consent to data collection and use practices. Second: the combined effect of all the individual decisions is an acceptable overall tradeoff between privacy and the benefits of collecting and using consumers' data. There are (we contend) decisive critiques of both claims. So why do policy makers and privacy advocates continue to endorse Notice and Choice?

Most likely, they see no need to seek an alternative. *We* find the critique of Notice and Choice conclusive, but our assessment is far from widely shared—and understandably so. Criticisms of Notice and Choice are scattered over several articles and books. No one has unified them and answered the obvious counterarguments. We do so. Making the critique plain, however, is not enough to ensure that policy makers turn to a viable alternative. The critiques are entirely negative; they do not offer any alternative to Notice and Choice. We offer an alternative: informational norms. When appropriate informational norms govern online data collection and use, they both ensure that visitors give free and informed consent to those practices, and yield an acceptable overall tradeoff between protecting privacy and the benefits of processing information. A fundamental difficulty is the lack of norms. Rapid advances in information processing technology have fueled new business models, and the rapid development has outpaced the slow evolution of norms. Notice and Choice cannot be pressed into service to remedy this lack. It is necessary to develop new norms.

Table of Contents

* Professor and Head, Department of Computer Science, University of Illinois at Chicago.
Partially supported by National Science Foundation Grant No. DGE-1069311.
** Professor of Law, Chicago-Kent College of Law, Visiting Foreign Professor, University of Gdańsk, Poland.

Informational privacy is the ability to determine for yourself when others may collect and how they may use your information.[1] Adequate informational privacy requires a sufficiently broad ability to control collection and use, and this requires a sufficiently broad ability to give or

[1] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967). *See also* JAMES B. RULE, PRIVACY IN PERIL: HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE 3 (2007) (defining privacy "as the exercise of an authentic option to withhold information on oneself"); Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1462 (2000) ("I will use 'informational privacy' as shorthand for the ability to control the acquisition or release of information about oneself"); Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 763 (1989) ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person").

withhold free and informed consent to proposed collections and uses; otherwise, you cannot determine *for yourself* what others do with your information.[2]

Notice and Choice (sometimes called Notice and Consent[3]) is the current paradigm for securing free and informed consent to business's online data collection and use practices.[4] The "notice" is a presentation of terms. The "choice" is an action signifying acceptance of the terms (typically using the site or clicking on an "I agree" button).[5] When the notice contains information about a business's data collection and use, the argument for Notice and Choice rests on two claims. First: when adequately implemented, Notice and Choice ensures that website visitors can give free and informed consent to businesses' data collection and use practices. Second: the combined effect of the individual consent decisions is an acceptable overall tradeoff between privacy and the benefits of information processing.[6] There are well-known, compelling

[2] We do not distinguish between personally identifying information (PII) and non-PII, because recent advances in de-anonymization ensure that, in many cases, non-PII may in fact identify individuals. *See, e.g.*, Arvind Narayanan & Vitally Shmatikov, *Robust De-anonymization of large sparse datasets*, *in* PROCEEDINGS OF THE IEEE SYMPOSIUM ON SECURITY AND PRIVACY 111–125, 111 (2008); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1814 (2011); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

[3] *See, e.g.*, Fred Cate, *The Failure of Fair Information Practice Principles*, *in* THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES 342, 351 (Jane Winn ed., 2006); and Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, *in* PROCEEDINGS OF THE ENGAGING DATA FORUM: THE FIRST INTERNATIONAL FORUM ON THE APPLICATION AND MANAGEMENT OF PERSONAL ELECTRONIC INFORMATION (2009), http://senseable.mit.edu/engagingdata/downloads.html.

[4] For a recent description and endorsement of notice and choice, see FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), http://www.ftc.gov/opa/2012/03/privacyframework.shtm (last visited Sep 26, 2012)(presenting a version of Notice and Choice that relies heavily on context and voluntary or legislative restrictions on data collection and use). For additional references, see *infra* note 8.

[5] As Paul Schwartz notes, "when a Web site says something about its data processing practices—even if this statement is vague or reveals poor practice—the visitor to the site is deemed to be in agreement with these practices so long as she sticks around. This summary, despite its ironic tone, is no exaggeration." Paul Schwartz, *Internet Privacy and the State*, 22 CONN. L. REV. 815, 82425 (2000).

[6] The tradeoff claim is rarely explicit in the literature arguing for Notice and Choice. *See infra* text accompanying notes 37 – 40.

critiques of both claims.[7] Policy makers and privacy advocates nonetheless typically insist on adherence to Notice and Choice.[8] The Federal Trade Commission, for example, recently endorsed it and provided guidelines for its implementation.[9]

[7] An early and influential critique is Paul Schwartz, *supra* note 6 (Notice and Choice does not ensure free choice because of information asymmetries, collective action problems, limited rationality, and a lack of market options). More recent critiques include: MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013) (Notice and choice as implemented is inconsistent with the requirements of free choice); COMMENTS OF THE CENTER FOR DIGITAL DEMOCRACY AND U.S. PIRG, IN THE MATTER OF A PRELIMINARY FTC STAFF REPORT ON PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 33 (2011), http://www.ftc.gov/os/comments/privacyreportframework/00338-57839.pdf ("Informed consent in the digital marketing era requires . . . a new commitment to candor and honesty . . . [the online marketing industry] needs to clearly explain to the user how the data are collected and used"); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DEDALUS 32, 36 (2011) (noting "the transparency paradox. Achieving transparency means conveying information handling practices [however] If notice . . . finely details every [relevant fact] . . . 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," and arguing for a much greater reliance on context); Barocas and Nissenbaum, *supra* note___ (consumers "confront . . . full-on barriers to achieving meaningful understanding of the practice and uses to which they are expected to be able to consent."); Paul M. Schwartz & Daniel Solove, *Notice and Choice: Implications for Digital Marketing to Youth*, (2009), http://digitalads.org/documents/Schwartz_Solove_Notice_Choice_NPLAN_BMSG_memo.pdf (Notice and Choice fails to ensure a free choice and fails to ensure an informed choice) ; Cate, *supra* note 3 at 369 ("as transposed into contemporary privacy laws and regulations, FIPPS [Fair Information Privacy Practices] have been used to glorify individual choice as if that, and not appropriate privacy protection, were the goal of data protection. While privacy advocates and policymakers cling tenaciously to FIPPS, at least in their rhetoric, the reality is that FIPPS as applied today largely disserve both privacy and other important societal interests"); J. Howard Beales III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, U. CHI. L. REV. 109–135, 114 (2008) ("The reality that decisions about information sharing are not worth thinking about for the vast majority of consumers contradicts the fundamental premise of the notice approach to privacy"); RULE, *supra* note 1 (privacy advocates pay insufficient attention to how to balance privacy versus competing concerns).

[8] Notice and Choice has its roots in the formulation of the fair information practices in 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), http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm (formulating the fair information principles in Section III). The practices were later refined and expressed in terms of Notice and Choice in THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977), http://epic.org/privacy/ppsc1977report/; Fred Cate reviews the development of Notice and Choice in Cate, *supra* note 3. Additional books, articles, and reports endorsing some form of Notice and Choice include the following: FEDERAL TRADE COMMISSION, *supra* note 2; U.S. DEPARTMENT OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY

A somewhat unsympathetic but not entirely inapt analogy is the old joke about the drunk and the streetlight:

> A policeman sees a drunk man searching for something under a streetlight and asks what the drunk has lost. He says he lost his keys and they both look under the streetlight. After a few minutes the policeman asks if he is sure he lost them here, and the drunk replies, no, that he lost them in the park. The policeman asks why he is searching here, and the drunk replies, "This is where the light is."[10]

Policy makers and privacy advocates search under streetlight of Notice and Choice even though consent not there. Why don't they look in the "park"? Most likely, they see no need to do so. *We* find the critiques of Notice and Choice conclusive, but our assessment is far from widely shared—and understandably so. The criticisms are scattered over several articles and books.[11] No one has unified them and answered the obvious counterarguments. We do so. Making the critique plain, however, is not enough to move policy makers from the "streetlight" to the "park." The critiques are entirely negative; they do not point to an alternative, a "park" in which to search for consent. As Helen Nissenbaum notes, "Why exactly the existing transparency-and-choice, or notice-and-consent, approach has failed—and what to do about it—remains hotly disputed."[12]

We offer an alternative: informational norms. Informational norms are social norms that constrain the collection, use, and distribution of information. Such norms explain, for example,

---

FRAMEWORK (2010), http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework ("To promote informed consent . . . [a revitalized Fair Information Practices] should promote increased transparency through simple notices, clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes, and expanded use of robust audit systems to bolster accountability") ; Daniel J. Solove & Chris Jay Hoofnagle, *Model Regime of Privacy Protection, A*, U. ILL. L. REV. 357 (2006); NATIONAL ADVERTISING ALLIANCE, DRAFT CODE OF CONDUCT FOR PUBLIC COMMENT (2013), https://www.networkadvertising.org/Draft_NAI_Code_For_Public_Comment.pdf (arguing for more effective, contextually presented notices and requiring opt-in for sensitive data).

[9] FEDERAL TRADE COMMISSION, *supra* note 4.

[10] Adapted from DAVID H. FREEDMAN, WRONG: WHY EXPERTS KEEP FAILING US (2010).

[11] *See infra* Section I.

[12] Nissenbaum, *supra* note 7 at 34–35.

why your pharmacist may inquire about the drugs you are taking, but not about whether you are happy in your marriage. When appropriate norms govern online exchanges, they ensure that visitors give free and informed consent, and they also implement an acceptable tradeoff between privacy and competing concerns.

Critiques are most effective when they undermine their targets' strongest points; accordingly, we begin with a review of the arguments *for* Notice and Choice. Discussions of Notice and Choice typically pay little, if any, explicit attention to its underlying rationale,[13] so our review sometimes, of necessity, extrapolates arguments as much as it reports them. We present these arguments in Section I. Section II contains our critique of Notice and Choice. We present our norm-based alternative in Section III and conclude in Section IV will a call to study norms and their role in ensuring free and informed consent.

I. The Allure of Notice and Choice

The allure of Notice and Choice is that it appears with one elegant stroke to ensure that consent is informed and free and *thereby* also to implement an acceptable tradeoff between privacy and competing concerns.[14] We start with the argument that Notice and Choice secures informed consent.

[13] Noteworthy exceptions include RADIN, *supra* note 7; RULE, *supra* note 1.

[14] Paul Schwartz and Daniel Solove note that Notice and Choice was initially adopted in response to the promulgation of the Fair Information Practices (FIPs). Those practices require "(1) transparency of record systems, (2) collection and use of information that is accurate, relevant, and up to-date (data quality principle), (3) notice about what information was being collected about individuals, (4) a right to prevent information collected for one purpose from being used for other purposes, (5) a right to access one's personal information, (6) a right to correct erroneous information, and (7) data security protections." They contend that "In contrast to Europe, where the FIPs were highly influential and led to omnibus privacy protections, the United States has adopted a more market-driven approach toward regulating consumer privacy. Businesses and marketers pushed the notice and choice approach, which selectively adopts only a few FIPs. Only the third FIP listed above survives in the notice and choice approach. The fourth FIP – often

A. Informed Consent: The Role of Notices

A website visitor's consent to a business's data collection and use practices is informed if the visitor has sufficient knowledge of the practices to make a reasonable evaluation of the risks and benefits of disclosing information. The required information is typically taken to be an adequate amount *specific detail* about the type of data collected, the purposes for which it is used, and the third parties with which it is shared.[15] Proponents and critics of Notice and Choice share this *specificity assumption*.[16] We will reject it later,[17] but we grant it for now. The problem is that visitors generally have little knowledge of the ways in which online businesses collect and use information.[18] Notice and Choice offers an obvious solution: present visitors with the necessary information. The almost universal practice online is to make the presentation in a standard form contract. The relevant information may be scattered across multiple documents—a privacy policy, a terms of use agreement, a sales agreement, and so on. Whether in one document or several, we will call the totality of the written terms addressing data collection and use a "Notice." As long as the Notice sufficiently describes the practices, a visitor who reads and understands it has sufficient knowledge of those practices.

---

referred to as the purpose-specification principle – is recast as 'choice.'" Schwartz and Solove, *supra* note 2 at 1.

[15] See Cate, *supra* note 3 (reviewing Notice and Choice requirements).

[16] Among proponents, *see, e.g.*, FEDERAL TRADE COMMISSION, *supra* note 4; Among critics, *see, e.g*, Nissenbaum, *supra* note 7 at 36.

[17] *See infra* Section III,C.

[18] *See* FEDERAL TRADE COMMISSION, *supra* note 4 at 79 (noting that "one of the major themes of the roundtables is that consumers lack understanding of various data practices and their privacy implications, and thus lack the ability to make informed decisions about the trade-offs involved"). *See also* Jeff Chester, *CookieWars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the "Big Data" Era*, *in* EUROPEAN DATA PROTECTION: IN GOOD HEALTH? 53–77 (Serge Gutwirth et al. eds., 2012).

This obvious solution prompts an equally obvious objection: the vast majority of visitors do not read Notices.[19] So doesn't it follow that the vast majority of visitors fail to give informed consent?[20] No, not as long as *hypothetical* knowledge counts as sufficient for informed consent. The relevant hypothetical knowledge is the knowledge a visitor would gain from reading the Notice. Counting the hypothetical knowledge as sufficient for informed consent is precisely what courts do. They invoke the duty to read: as long as a party has an adequate opportunity to read and understand an agreement, then the court deems the party to know the terms of the agreement even if he or she did not read it.[21] Thus, if a visitor has an adequate opportunity to read and understand a Notice, a court will deem the visitor to know what it says, and—provided the Notice sufficiently describes the business's data collection and use practices—the visitor's consent will count as informed.

The duty is a special case of the following widely accepted normative principle: if you know that, with reasonable time and effort, you could obtain information relevant to a future action, and you freely choose not to obtain that information, then, within broad limits, when you act, you assume the risk of adverse consequences of which you would have been aware and which you could have avoided had you obtained the information. This is why "[i]t will not do for a man to enter into a contract, and, when called upon to abide by its conditions, say that he did

[19] S*ee e.g.*, Beales and Muris, *supra* note 7. With regard to standard form contracts generally, "[t]he fact that consumers do not read standard form contracts is so well accepted and documented as to be virtually enshrined as dogma within the contracts literature." Wayne Barnes, *Toward A Fairer Model Of Consumer Assent To Standard Form Contracts: In Defense Of Restatement Subsection 211(3)*, 82 WASH. L. REV. 227, 237 (2007). *See also* R. A Hillman, *Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?*, 104 MICH. L. REV. 837–856 (2006).

[20] RADIN, *supra* note 7.

[21] "One having the capacity to understand a written document who reads it, or, without reading it or having it read to him, signs it, is bound by his signature." JOSEPH PERILLO, 7 CORBIN ON CONTRACTS 402 –403 (rev. 2002 ed.).

not read it when he signed it, or did not know what it contained."[22] Despite its normative pedigree, the duty to read has caused considerable academic concern.[23] We nonetheless assume for the sake of argument that the "duty to read interpretation" of informed consent is correct. Our point, which we will develop in Section II, is that Notice and Choice fails to ensure informed consent even when we grant that hypothetical knowledge is sufficient to make consent informed.

B. Free consent: Affirmative Act or Passive Acquiescence?

Courts treat Notices as contracts, and, as Mark Lemley notes, "[a]ssent by both parties to the terms of a contract has long been the fundamental principle animating contract law. Indeed, it is the concept of assent that gives contracts legitimacy and distinguishes them from private legislation."[24] A private party does not have the power to *unilaterally* impose legally enforceable obligations on other adult parties. Only governments can legitimately exercise such power. Special circumstances aside, the only way a private party can impose legally enforceable terms on another adult party is to secure that party's free assent to being bound.

Margaret Jane Radin offers a useful characterization of when consent is free. Free consent "requires [1] a knowing understanding of what one is doing [2] in a context in which it is actually possible for one to do otherwise, and [3] an affirmative action in doing something, rather than a merely passive acquiescence in accepting something."[25] In her book, *Boilerplate*, Radin

[22] Sanger v. Dunn, 3 N. W. 388, 389 (1879).
[23] *See* Barnes, *supra* note 19 (citing and discussing the extensive duty to read literature).
[24] Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 464–65 (2006).
[25] Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1126 (1999).

argues that only actual knowledge can fulfill the "knowing understanding" requirement,[26] and she concludes that visitors' consent is not free on the ground that non-reading visitors have only hypothetical knowledge of the terms in Notices. As important as it is, we will not pursue this point. We grant for the sake of argument that hypothetical knowledge fulfills the "knowing understanding" requirement. Our critique is that it is still problematic to regard consent as free. The background for that critique is the following argument in favor of the claim that consent is free. An example is helpful.

Imagine Vicky visits Amazon.com to buy a book. Two points are clear. She has (as we have granted) a knowing understanding of Amazon's privacy practices.[27] Further, the context is clearly one in which "it is actually possible . . . to do otherwise." She is under no compulsion to use Amazon. She could buy books from Barnes and Noble's website, or not buy books online at all. The critical question concerns the final condition: Is her visit to Amazon's website "an affirmative action in doing something, rather than a merely passive acquiescence in accepting something"? It certainly *looks* like an affirmative action. It is an informed decision to exchange the data about herself that Amazon collects for the book-buying service Amazon provides, a service she is under no compulsion to use. Vicky would not engage in this exchange if she did not judge that the service was worth more to her than her withholding her data. Her "worth more" judgment may be affected by various cognitive biases (over-discounting future risks, for example), but, if so, this just shows that her judgment poor, not that her action is unfree.[28] Free choices can be bad choices. But bad or good, if Vicky chooses because she finds the service

[26] RADIN, *supra* note 7.
[27] Vicky has at least the hypothetical knowledge contained in Amazon.com, AMAZON.COM PRIVACY NOTICE, http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496#gather.
[28] OWEN BAR-GILL, SEDUCTION BY CONTRACT: LAW, ECONOMICS, AND PSYCHOLOGY IN CONSUMER CONTRACTS (2012).

worth more to her than not disclosing her data, how can the action be mere passive acquiescence?

C. Summing to an Acceptable Tradeoff

Living in a highly digitized society entails a tradeoff between informational privacy and the benefits of information processing. The credit system is a good example. The billions of credit, debit, and bank cards testify to consumers' embrace of the system, which does indeed offer significant benefits.

> The expansion of credit reporting, along with improvements in credit scoring, has facilitated substantial expansion in the availability of credit to American consumers, as well as the democratization of credit. Credit grantors can make more expeditious decisions, often without a personal visit to a loan officer, enabling the phenomenon of "instant credit" and offering significant benefits to consumers as a group.[29]

Consumers opt for the benefits even though, "[u]nlike many other countries, credit reporting in the US is 'full file' or 'comprehensive' reporting, including both positive and negative information about consumers."[30] In general, studies show that consumers find it acceptable to give up some degree of privacy to get the benefits of information processing. As Harris Poll reports,

> almost two-thirds of all adults (64%) are . . . often willing to allow people to have access to, and to use, their personal information where they understand the reasons for its use, where they see tangible benefits for so doing and when they believe care is taken to prevent the misuse of this information.[31]

[29] Beales and Muris, *supra* note 7 at 115–16.
[30] *Id.* at 115.
[31] Humphrey Taylor, *Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefit*, 17 THE HARRIS POLL (2003), http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf (last visited Nov 8, 2012).

Of course, not just any tradeoff will do. Consumers want an acceptable one. So what counts as acceptable?

An adequate answer requires a clear conception of the benefits and risks. Commentators commonly identify the following benefits: increased economic efficiency, improved security, better personalization of services, increased availability of relevant information, and innovative platforms for communication.[32] Realizing the benefits requires relinquishing at least some degree of control over one's information and thus entails a loss of informational privacy. Thus, it is routine to take the loss of informational privacy as the sole, or at least the most important, risk. This "one" risk, however, includes a variety of specific consequences. "Theorists have proclaimed the value of privacy to be protecting intimacy, friendship, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, thought, democracy, reputation, and psychological well-being."[33] Despite the complex consequences that flow from reducing privacy, this picture of the tradeoff

[32] *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193–1294 (1998) (emphasizing availability of relevant information, increased economic efficiency, improved security); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75 (2008) ("policy decisions frequently counterpose privacy against two other powerful values: efficiency and security"); For consumer willingness to trade privacy for various benefits, see Taylor, *supra* note 31; PREFERENCECENTRAL, CONSUMER PERSPECTIVES ON ONLINE ADVERTISING - 2010 (2010), http://www.preferencecentral.com/consumersurvey/download/(arguing that "over half of consumers surveyed indicated that they prefer relevant targeted online ads as a trade-off for access to free content"); and ; CHOICESTREAM, 2006 CHOICESTREAM PERSONALIZATION SURVEY, http://www.choicestream.com/pdf/ChoiceStream_PersonalizationSurveyResults2006.pdf (claiming that only fifteen percent of web users would give up personalization benefits to avoid revealing personal details); compare JOSEPH TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT (2009), http://ssrn.com/abstract=1478214 (arguing that the vast majority of consumers find behavioral advertising unacceptable). The opposing studies illustrate the well-known truth about surveys: what you ask determines what you get. The most reasonable interpretation of the surveys is that consumers reject the current privacy/efficiency tradeoff and want a tradeoff that gives them more control over their privacy.

[33] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 98 (2008). *See also* John Collette, *Role Demands, Privacy and Psychological Well-Being*, 30 INTERNATIONAL JOURNAL OF SOCIAL PSYCHIATRY 222 (1984).

problem is not particularly complex: a relatively short list of benefits competes against the value of informational privacy. Recent developments necessitate a much more complicated picture, as we argue later,[34] but we stay with the simpler picture for the moment.

Even with the simple picture, the balancing task is immense. The benefits and risks affect society as whole. Increasing the availability of relevant information and innovative platforms for communication may, for example, yield a better informed and more politically involved citizenry. Increasing privacy risks may create a chilling effect that stunts rather than encourages the free exchange of ideas and opinions. Improving the personalization of services requires collecting, analyzing, and retaining information that may be also be used for a variety of other purposes—to engage in price discrimination, or to determine whether someone qualifies for a credit card, mortgage, health insurance, or appointment as a Supreme Court Justice, for example. Price discrimination, the extension of credit, the distribution of health insurance, and the composition of the Supreme Court determine in part which segments of society have access to what goods and services, and that distribution of goods and services has long-term effects on the type of society that evolves, and on whether it distributes benefits and imposes risks fairly.

Ideally, an acceptable balance is one that cannot be improved, one that is at least as good as any other possible balance. The balancing task is so complex that practice only approximates the ideal, and the sensible demand is for a sufficiently close approximation the ideal. The balancing task is further complicated by the fact that disagreement on balancing questions is the order of the day. As James Rule remarks, "we cannot hope to answer [complex balancing questions] until we have a way of ascribing weights to the things being balanced. And, that is exactly where the parties to privacy debates are most dramatically at odds."[35] Disagreements

[34] *See infra* Section II,A,3.
[35] RULE, *supra* note 1 at 183.

about balancing issues in the privacy context are just a special case of disagreement about questions of social justice generally. As John Rawls emphasizes,

> reasoned and uncoerced agreement are not to be expected . . . Our individual and associative points of view, intellectual affinities and affective attachments, are too diverse . . . to allow of lasting and reasoned agreement. . . [The appropriate view of social organization] takes deep and unresolvable differences on matters of fundamental significance as a permanent condition of human life.[36]

Notice and Choice appears to offer an appealing way to deal with "deep and unresolvable differences on matters of fundamental significance."

To see why, consider first that the overall pattern of giving or withholding consent does indeed draw a line between permissible and impermissible uses of information. It is a complex line varying with the vagaries of consent, but it is a line nonetheless, and, as such, it defines a complex and varying tradeoff between the benefits of processing information and the need to protect informational privacy. Merely to define a tradeoff is of course not necessarily to define an *acceptable* one. An acceptable tradeoff has to adequately balance the benefits and risks to society as a whole. But why shouldn't the individual consent decisions sum to precisely, or at least approximately, that balance? If each person gives free and informed consent to the tradeoffs that are acceptable to that person, why should not the overall result of all such decisions be an acceptable tradeoff for society as a whole?

As we argue later, there is very little reason to it will.[37] However, the *only* tradeoff mechanism we can find in the Notice and Choice literature is the combined effect of the individual consent decisions, so we take a commitment to this approach to be implicit it in the literature's endorsement of Notice and Choice. For the most part, proponents of Notice and

[36] John Rawls, *Kantian Constructivism in Moral Theory*, 77 THE JOURNAL OF PHILOSOPHY 515–572, 534 (1980).
[37] *See infra* Section II, A.

Choice do not explicitly address the tradeoff problem.[38] However, as Paul Schwartz and Daniel Solove note, "The idea behind notice and choice can be summarized in this fashion: As long as a company provides notice of its privacy practices, and people have some kind of choice about whether to provide the data or not, then privacy is sufficiently protected."[39] Schwartz and Solove do not provide any gloss on what they regard as "sufficiently protected," but, on any view that recognizes the need to balance the value of privacy against the benefits of information processing, privacy is not protected in the right way if the overall tradeoff is unacceptable.[40]

II. The Critique

Our critique is that Notice and Choice ensures neither free nor informed consent; nor does it yield an acceptable tradeoff. We begin with the argument that consent is not informed.

[38] For example, one of the Federal Trade Commission's earlier endorsements of Notice and Choice came in FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf; Commission Swindle in dissent sharply criticized the report for its lack of attention to tradeoff questions, "The Privacy Report fails to pose and to answer basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could severely stifle the New Economy. Shockingly, there is absolutely no consideration of the costs and benefits of regulation; nor the effects on competition and consumer choice; nor the experience to date with government regulation of privacy; nor constitutional implications and concerns; nor how this vague and vast mandate will be enforced."ORSON SWINDLE, DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE IN PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE A REPORT TO CONGRESS, http://www.ftc.gov/reports/privacy2000/swindledissent.pdf; Unfortunately, it is common for proponents of Notce and Choice to over-emphasize consent and ignore important tradeoff issues. See Cate, *supra* note 3 at 361–367.

[39] Schwartz and Solove, *supra* note 7 at 1.

[40] In his excellent book, *Privacy in Peril*, James Rule seems in the end to endorse the claim that the combined effect of informed consent decisions yields an acceptable tradeoff. He recommends that in "the private sector [the following] precept should apply: no use of personal data for institutional surveillance without meaningful informed consent from the individual." RULE, *supra* note 1 at 196. Rule notes that this precept would alter the existing tradeoff between privacy and a variety of competing concerns, and he endorses the change.

A. It Is Impossible for a Notice to Contain Enough Information

A visitor's consent is informed if he or she has sufficient knowledge of the practices to make a reasonable evaluation of the risks and benefits of disclosing information. Notice and Choice claims to remedy visitors' lack of knowledge of data collection and use practices by presenting sufficient information in a Notice. The criticism is that it is *impossible* for a Notice to contain enough information. The argument turns on two facts. First, current data collection practices are extremely complex. Second, these practices collect information on one occasion for one purpose and then retain, analyze, and distribute it for a variety of other purposes in unpredictable ways. We start with the complexity point.

1. Complexity

Websites feed information to a complex ecosystem that tracks consumers' online activities in order to deliver tailored advertising.[41] We offer a simplified model consisting of only five entities: profilers, advertising agencies, advertising exchanges, websites that display the advertisements, and businesses that purchase the advertisements.[42] Profilers segment buyers into groups to predict their willingness to buy.[43] eXelate, for example, collects information about age, sex, ethnicity, marital status, profession, Internet search information, and information

[41] *See, e.g.*, FEDERAL TRADE COMMISSION, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), www.ftc.gov/os/2009/02/P085400behavadreport.pdf; COMMENTS OF THE CENTER FOR DIGITAL DEMOCRACY AND U.S. PIRG, *supra* note 7; Schwartz and Solove, *supra* note 7.

[42] Models may distinguish several more entities and functions. For example, some make a subtle distinction between advertising networks and advertising exchanges. *See, e.g.*, *Data Usage & Control Primer: Best Practices & Definitions*, INTERACTIVE ADVER. BUREAU 12 (2010), http://www.iab.net/media/file/data-primer-final.pdf.

[43] *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 425, 462-64 (2011).

about sites visited.[44] The purpose of the profiles is to target text and display advertising.[45] Advertising exchanges, such as Google's AdSense, deliver advertisements to the websites that display them.[46] When a visitor arrives at a website, an advertising exchange combines the visitor's profile with information about his or her current website activity in order to more precisely target advertisements.[47] The exchange then conducts an auction in which businesses bid for the opportunity to present their targeted advertisements (the whole process takes milliseconds).[48] The complexity is immense. As Helen Nissenbaum says,

> 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 . . . 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.[49]

Nissenbaum concludes that "the complexity makes it not only difficult to convey what practices are followed and what constraints respected, but practically impossible."[50] This follows given the *specificity assumption* we noted in the last section: to provide enough knowledge for an informed decision, a Notice must contain an adequate amount *specific detail* about the type of

---

[44] *See* Emily Steel, *Exploring Ways to Build a Better Consumer Profile*, WALL ST. J., Mar. 15, 2010, http://online.wsj.com/article/SB10001424052748703447104575117972284656374.html.
[45] *See* Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 4 (2011) ("These profiles allow websites and ISPs to serve advertisements and other services that are targeted to their customers' interests.").
[46] *See AdSense Basics*, GOOGLE, http://support.google.com/adsense/bin/answer.py?hl=en&answer=9712 (last visited Sept. 21, 2012).
[47] *See* Schwartz and Solove, *supra* note 2 at 1851–1852.
[48] *See id.* at 1852.
[49] Nissenbaum, *supra* note 7 at 35–36. *See also* CENTER FOR DIGITAL DEMOCRACY, IN THE MATTER OF REAL-TIME TARGETING AND AUCTIONING, DATA PROFILING OPTIMIZATION, AND ECONOMIC LOSS TO CONSUMERS AND PRIVACY (2010), http://www.centerfordigitaldemocracy.org/sites/default/files/20100407-FTCfiling.pdf (discussing in detail the complexity of the online advertising ecosystem).
[50] Nissenbaum, *supra* note 7.

data collected, the purposes for which it is used, and the third parties with which it is shared. This is why Nissenbaum asks one to "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."[51] The system is so complex that any attempt to trace what information is collected, the purposes for which it used, and where it goes is "so complicated that probably only a handful of deep experts would be able to piece together a full account."[52] This makes it difficult to make a Notice sufficiently informative. It is practically impossible because the advertising ecosystem has a "recursive capacity that is indefinitely extensible"[53] so that even an accurate "snapshot of the information flows"[54] is valid only for a short time.

The inference from complexity to impossibility leans heavily on the specificity assumption requirement that a Notice must provide sufficient detail about the workings of the current advertising ecosystem. The next impossibility argument, based on long-term data retention, does not assume that a Notice must contain specific details beyond merely identifying the purposes for which collected information is used.

2. Long-term retention

The advertising ecosystem collects information for one purpose and retains it for use for other unpredictable purposes in the future. The retention of data for unpredictable future purposes means the Notice would have to contain information no one knows. As Daniel Solove observes,

> An individual may give out bits of information in different contexts, each transfer appearing innocuous. However, the information can be aggregated and could prove to be invasive of the private life when combined with other information . . . From the

[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*

> standpoint of each particular information transaction, individuals will not have enough facts to make a truly informed decision. The potential future uses of that information are too vast and unknown to enable individuals to make the appropriate valuation.[55]

One cannot put in a Notice what one does not know.

In light of the one-two punch of complexity and long-term data retention, one may well wonder how Notice and Choice has survived as long as it has as seriously advocated policy. The answer is that proponents of Notice and Choice typically argue for restrictions on data collection and use that greatly reduce both complexity and long-term data retention. The Federal Trade Commission, for example, insists that "companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law."[56] The Commission also demands that companies "implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected."[57]

We think minimizing data collection is unwise and unrealistic. Our arguments appeal to the fact that "[w]e live in the age of Big Data."[58]

3. Big Data and its implications

"Big data" refers to the acquisition and analysis of massive collections of information, collections so large that until recently the technology needed to analyze them did not exist.[59]

---

[55] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393–1462, 1452 (2001).
[56] FEDERAL TRADE COMMISSION, *supra* note 4 at 27. *See also infra* note 8.
[57] *Id.* at 28. The FTC is hardly alone in its insistence on Notice and Choice combined with significant restrictions on data collection and retention. The European Union takes a similar approach. Solove and Hoofnagle, *supra* note 8; RULE, *supra* note 1.
[58] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364 (last visited Oct 29, 2012).
[59] Omer Tene & Jules Polonetsky, *Privacy In The Age Of Big Data: A Time For Big Decision*, 64 STAN. L. REV. ONLINE 63 (2012).

The key point here is that analyzing massive collections of data reveals patterns that would otherwise go unnoticed.[60] The analysis often requires analyzing data collected and retained over long periods of time. This is why the "big data business model is antithetical to data minimization. It incentivizes collection of more data for longer periods of time. It is aimed precisely at those unanticipated secondary uses, the 'crown jewels' of big data."[61]

A well-known example is Dr. Russ Altman's discovered that taking the antidepressant Paxil together with the anti-cholesterol drug Pravachol could result in diabetic blood sugar levels.[62] He made two uses of big data. He obtained a symptomatic footprint characteristic of very high blood sugar levels by analyzing thirty years of reports in the Federal Drug Administration's Adverse Event Reporting System database, and then found that footprint in the Bing searches using an algorithm that detected statistically significant correlations. People taking both drugs also tended to enter search terms ("fatigue" and "headache," for example) that constitute the symptomatic footprint.

This is not an isolated example. Big data analyses have reduced emergency room costs,[63] improved the treatment for cystic fibrosis, created life-saving treatment for premature babies,[64] helped combat polio in Ethiopia,[65] improved access to social services in India by creating digital

[60] *See, e.g.*, Office of Science and Technology Policy, Executive Office of the President, OBAMA ADMINISTRATION UNVEILS "BIG DATA" INITIATIVE: ANNOUNCES $200 MILLION IN NEW R&D INVESTMENTS (2012), http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release.pdf ("By improving our ability to extract knowledge and insights from large and complex collections of digital data, the initiative promises to help solve some the Nation's most pressing challenges").
[61] Tene and Polonetsky, *supra* note 59 at 22.
[62] Tene and Polonetsky, *supra* note 58.
[63] RICK SMOLAN & JENNIFER ERWITT, THE HUMAN FACE OF BIG DATA 34 (2012).
[64] *Id.* at 65.
[65] *Id.* at 113.

IDs,[66] and improved police response times by using acoustic sensors to detect and triangulate the sound of gunfire.[67]

Such restrictions would also be unwise. Adopting them mean turning our backs on the benefits Big Data offers. Surely judicious balancing of risks and benefits is better. Accordingly, we reject the restrictions that would be required to give Notices a reasonable chance of being sufficiently informative. In any case, the big data genie is not about to go back in the bottle.[68] Suggesting the imposition of severe restrictions on data collection and retention is about as realistic as shouting at a tidal wave that it should stop.

B. How Can Consent Be Anything But Passive Acquiescence?

The argument *against* Vicky's use of Amazon being passive acquiescence was that she regards using Amazon as worth more to her than surrendering her data. The problem is that it does not follow from the "worth more" judgment that her use is not mere passive acquiescence. Compare a thief who, with a gun to your head, demands, "Your money or your life!" You hand over the money because you regard your life as being worth more than the money, but, if anything is a case of passive acquiescence, you handing over the money is. There is no gun to Vicky's head, but her choice is also highly constrained. She could use a different online book seller—Barnes and Noble, for example, but Barnes and Noble's practices are very similar to

[66] *Id.* at 72.
[67] *Id.* at 87.
[68] *See* IAN AYRES, SUPER CRUNCHERS: WHY THINKING BY NUMBERS IS THE NEW WAY TO BE SMART (2007). Nate Silver expresses some well justified caution. NATE SILVER, THE SIGNAL AND THE NOISE: WHY SO MANY PREDICTIONS FAIL — BUT SOME DON'T 9 – 12 (2012). The book as a whole, however, illustrates that Big Data has come of age. *See also* Tene and Polonetsky, *supra* note 58; SMOLAN AND ERWITT, *supra* note 63; BARRY DEVLIN, SHAWN ROGERS & JOHN MYERS, BIG DATA COMES OF AGE (2012), http://www.9sight.com/Big_Data_Comes_of_Age.pdf.

Amazon's.[69] Indeed, virtually all online sellers collect and use a significant amount of data.[70] Vicky could of course only buy books from brick and mortar bookstores, but such stores are disappearing, and the ones that remain carry only a limited inventory. In any case, Vicky wants the convenience of online shopping. She could research online sellers' Notices to find those most consistent with her privacy preferences, but she is not willing to spend that much time and effort. She is already committed to a variety of goals—raising her children, pursuing her career, enjoying her friends, and so on—and the time she is willing to allot to buying books is relatively brief. So agreeing to a seller's data collection practices is her only viable option.

It does *not* follow however that Vicky's consent is not free. The gun to the head example notwithstanding, highly constrained choices can in some cases still be free. Imagine, for example, that your dream vacation is to go to the Cayman Islands. Your budget makes the trip impossible unless you opt for an "all inclusive" vacation package that offers airfare, hotel, and food for a single affordable price. When you sit down to eat the food, your choice is highly constrained (your options being go hungry or spend money you cannot afford), but, unlike the thief's demand, the constraint is not a profound and wholly unjustified interference with your pursuit of plans and projects which you value and to which you are committed. It is just the opposite; the constraint is a means that you *freely* choose in order to realize your vacation goal. You eat the food freely in the sense that doing so is a fully justified component of a freely chosen overall plan. This is a common pattern. You may have no practical option other than driving your children to daycare. You have to work; there is no one to care for them at home; and so on.

[69] Compare Amazon.com, *supra* note 14 to Barnes and Noble, PRIVACY PRINCIPLES, http://www.barnesandnoble.com/help/cds2.asp?PID=25556.

[70] *See* Felicia Williams, *Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles*, FED. TRADE COMM'N (2006), http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf ("The vast majority of the privacy policies stated the firms have the right to share any data with any third party for any reason.").

But your driving them to daycare is part of the pursuit of the freely adopted project of raising your children and as such it is not passive acquiescence but an affirmative action.

When Vicky buys from Amazon, is her constrained choice more like the gun to the head example or the daycare and Cayman Island examples? Schwartz and Solove evidently believe it is more like the gun to the head. They contend that

> the "choice" presented is more of a Hobson's choice than a real one. Many companies present consumers with a take-it-or-leave-it choice that provides hardly any ability for consumers to bargain about their privacy preferences. If a consumer wants to buy a product, read a website, subscribe to a magazine, use a service, and so on, the consumer can be forced either to surrender privacy or to go elsewhere. But when nearly all companies offer the same take-it-or-leave-it approach, consumers desiring to protect their privacy have nowhere to turn.[71]

Similarly, Todd Rakoff contends that "The consumer's experience of modern commercial life is one not of freedom in the full sense posited by traditional contract law, but rather one of submission to organizational domination, leavened by the ability to choose the organization by which he will be dominated."[72]

In section III, we argue that Schwartz, Solove, and Rakfoff are half right: in some cases website visitors' "Choices" are passive acquiescence; some are not.

C. Notice and Choice Leads to Unacceptable Tradeoffs

The Notice and Choice tradeoff claim is that if each person gives free and informed consent to the tradeoffs that are acceptable to that person, the overall result is some reasonably close approximation to an ideally acceptable tradeoff. It is extremely unlikely that this is true. Our argument distinguishes two tradeoff problems. First is the *simple problem*, which is the problem we described earlier. The benefits are increased economic efficiency, improved

[71] Schwartz and Solove, *supra* note 7.
[72] Todd Rakoff, *Contracts of Adhesion: An Essay In Reconstruction*, 96 HARV. L. REV. 1173, 1230 (1983).

security, better personalization of services, increased availability of relevant information, and innovative platforms for communication. The risk is the loss of informational privacy. The second problem, the *real tradeoff problem,* involves a greatly expanded range of risks and benefits. Notice and Choice fails to solve the simple problem and even more clearly fails to solve the real problem.

1. The simple tradeoff problem

Recall our earlier argument *in favor* of the Notice and Choice solution to the simple tradeoff problem. We concluded by asking, "If each person gives free and informed consent to the tradeoffs that are acceptable to that person, why shouldn't the overall result of all such decisions be an acceptable tradeoff for society as a whole?" The "It should" answer is actually far from plausible.

To begin with, there are many situations in which individuals' decision do not add up to an acceptable overall result. One famous example is the story of railway transportation to and from Ithaca, New York, a story that prompted the economist Alfred E. Kahn to write his famous article, *The Tyranny of Small Decisions: Market Failures, Imperfections, and The Limits of Economics*.[73] The last passenger train left Ithaca, New York in 1961.[74] Faced with the decision to travel by car, bus, air, or train, so many choose car, bus, or air that train service was no longer profitable and the railroad ceased to offer it even though it was the only reliable form of transportation in foul weather and in peak traffic conditions. Kahn suggests the discontinuance produced an unacceptable tradeoff:

[73] Alfred E. Kahn, *The Tyranny of Small Decisions: Market Failures, Imperfections, and The Limits of Economics*, 19 KYKLOS 23–47 (1966).
[74] Ithaca (New York), WikiTravel, http://wikitravel.org/en/Ithaca_(New_York).

> Suppose each person in the cities served were to ask himself how much he would have been willing to pledge regularly over some time period, say annually, by purchase of prepaid tickets, to keep rail passenger service available to his community. As long as the amount that he would have declared (to himself) would have exceeded what he actually paid on the period—and my own introspective experiment shows that it would—then to that extent the disappearance of the passenger service was an incident of market failure.[75]

Assuming, as Kahn does, that his reaction is representative, the lack of train service is unacceptable to most of those affected.

Notice and Choice is likely to produce a similar unacceptable result. The result in this case is the world Daniel Solove warns us we rapidly approach. He fears that we are

> heading toward a world where an extensive trail of information fragments about us will be forever preserved on the Internet, displayed instantly in a Google search. We will be forced to live with a detailed record beginning with childhood that will stay with us for life wherever we go, searchable and accessible from anywhere in the world. This data can often be of dubious reliability; it can be false and defamatory; or it can be true but deeply humiliating or discrediting. We may find it increasingly difficult to have a fresh start, a second chance, or a clean slate. We might find it harder to engage in self-exploration if every false step and foolish act is chronicled forever in a permanent record. This record will affect our ability to define our identities, to obtain jobs, to participate in public life, and more.[76]

Despite widespread disagreement about what counts as an acceptable tradeoff, we think most would find the world Solove envisions unacceptable. We think the combined effect of individual consent decisions is likely to lead to that world. We do so because we share James Rule's assessment of the plight of privacy:

> Ever-emerging technological possibilities and the ingenuity of planners generate a study stream of new ways of creating, capturing, and using personal data for one institutional purpose or another. And these innovations planned or accomplished pose one challenge after another to the privacy-protecting Davids, who mobilize thinly stretched resources against organizational Goliaths.[77]

[75] Kahn, *supra* note 73.
[76] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 17 (2007).
[77] RULE, *supra* note 1 at 144.

To make matters worse, there is a progressive "desensitization of publics to everyday demands on privacy. The sheer ubiquity of pressures for personal information, the variety of situations in which they occur, and the seeming lack of alternatives—all these things apparently conspire to create a sense that resistance is futile."[78] A sense of futility that results in acquiescence to increasing ever-increasing data collection and use is likely to lead the world in which "[w]e will be forced to live with a detailed record beginning with childhood that will stay with us for life wherever we go, searchable and accessible from anywhere in the world."

Even if that world does not become a reality, we find it hard to believe that the sum of individual consent decisions will yield an acceptable result. An acceptable tradeoff has to balance society-wide long-term effects. As James Rule notes, "any judgments about where and how to draw a line against endless, incremental erosion of privacy requires that most elusive of visions—a view of the whole."[79] Notice and Choice fails to incorporate an adequate view of the whole. Visitors have little understanding of businesses' data collection practices and of the attendant benefits. Why would individual decisions driven by individual concerns and based on whatever information is available at the time somehow add up an acceptable tradeoff? Even if Notices could, *per impossible*, contain all relevant information, and even if all visitors read and understood Notices, they would not have the information they need. The information required to adequately balance the benefits and risks concerns complex society-wide consequences that unfold over a long period of time. The lack of information problem becomes particularly severe when we turn to the complex real problem.

[78] *Id.* at 166.
[79] *Id.* at 144.

2. The real tradeoff problem

The simple tradeoff problem is no longer the actual problem. "Big data" is a primary reason. Big Data offers a much wider range of both risks and benefits than are present in the simple tradeoff. Our earlier examples are sufficient to illustrate the breadth of the benefits—from detecting drug interactions to reducing emergency room costs to improving police response times.[80] As even our very short list illustrates, the benefits are extraordinarily diverse. Moreover, one very important range of benefits is perhaps the one hardest to predict: new products and services. As the World Economic Forum has observed, personal data "will emerge as a new asset class touching all aspects of society."[81] The risks are equally broad and diverse. Big Data and Big Data analytics expand the range of possibilities, and making those possibilities realities typically creates both benefits and risks. The loss of informational privacy remains a key concern, but there is a wide range of other risks. For example, using digital IDs to improve access to social services in India will increase the demand for such services. Meeting the demand will mean an increased investment in those services, and that will have complex positive and negative effects on the Indian economy

The "view of the whole"[82] visitors need to make acceptable tradeoffs among such a complex array of benefits and risk far exceeds the view needed for the—already extremely difficult—task of balancing a short list of benefits against the loss of informational privacy. Visitors do not have the relevant information, nor do they generally have the expertise or experience required to make the complex tradeoffs involved. Thus, there is no reason to think that the individual consent decisions would sum to an acceptable outcome.

[80] *See infra* Section II,C, 3.
[81] WORLD ECONOMIC FORUM, PERSONAL DATA: THE EMERGENCE OF A NEW ASSET CLASS 5 (2011), http://www.weforum.org/reports/personal-data-emergence-new-asset-class (last visited Oct 29, 2012).
[82] RULE, *supra* note 1 at 146.

III. Beyond Notice and Choice

We see no acceptable way to rescue Notice and Choice. We think an alternative is necessary, and that informational norms provide it. Informational norms

> [g]enerally . . . circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed. In medical contexts, it is appropriate to share details of our physical condition or, more specifically, the patient shares information about his or her physical condition with the physician but not vice versa; among friends we may pour over romantic entanglements (our own and those of others); to the bank or our creditors, we reveal financial information; with our professors, we discuss our own grades; at work, it is appropriate to discuss work-related goals and the details and quality of performance.[83]

When informational norms govern online businesses data collection and use practices, website visitors give free and informed consent to acceptable tradeoffs.[84] Or rather, they do *as long as the norms have the property that we call being value-optimal*. We will first introduce the notion of value-optimality and then explain why, if there are value-optimal informational norms governing websites, then visitors give free and informed consent to acceptable tradeoffs. Our explanation is brief. So much so that we may seem open to Bertrand Russell's objection that "[t]he method of 'postulating' what we want has many advantages; they are the same as the

[83] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119–158, 120–121 (2004); A small sample of the diverse literature on norms includes HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); Jeroen van den Hoven, *Privacy and the Varieties of Informational Wrongdoing*, *in* READINGS IN CYBER ETHICS 430 (Richard A. Spinello & Herman T. Tavani eds., 2001); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STANDFORD LAW REVIEW 1373 (2000); Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW AND PHILOSOPHY 559–596 (1998); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999); MICHAEL PHILLIPS, BETWEEN UNIVERSALISM AND SKEPTICISM: ETHICS AS SOCIAL ARTIFACT (1994); PIERRE BOURDIEU & LOÏC J. D. WACQUANT, AN INVITATION TO REFLEXIVE SOCIOLOGY (1992); Roger Friedland & Robert R. Alford, *Bringing Society Back In: Symbolic Practices, and Institutional Contradictions*, *in* THE NEW INSTITUTIONALISM IN ORGANIZATIONAL ANALYSIS 232 (Walter W. Powell & Paul J. DiMaggio eds., 1991); James Rachels, *Why Privacy Is Important*, 4 PHILOSOPHY AND PUBLIC AFFAIRS 323 (1975); MICHAEL WALZER, SPHERES OF JUSTICE: A DEFENSE OF PLURALISM AND EQUALITY (1983).

[84] We discuss these matters in detail in ROBERT H. SLOAN & RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND INFORMATION SECURITY (2013).

advantages of theft over honest toil."[85] Our reply is that we are *neither* thieving *nor* toiling. We are indicating where to toil, indicating the "park" in which to look for free and informed consent.

A. Value-Optimality

A norm is value-optimal when, in light of the values of members of the group in which the norm obtains, the norm is at least as well justified as any alternative.[86] A norm that is at least as well justified as any alternative is either better justified than any alternative, or is tied with one or more alternatives that are also better than the rest. The point is that there is no *better* alternative. There are many optimality notions; Pareto optimality is perhaps the most well-known.[87]

Appeal to value-optimality allows us to define the ideal of *norm completeness*. Norm-completeness holds for transactions between visitors and online businesses when there is no significant tradeoff between privacy and competing goals that is not governed by at least one value-optimal informational norm.[88] Three further points about norm-completeness clarify its role.

---

[85] BETRAND RUSSELL, INTRODUCTION TO MATHEMATICAL PHILOSOPHY 71 (1920).

[86] We do not mean to suggest that people *explicitly* think that conformity to the norm is at least as well justified as any alternative. Typically, people just unreflectively conform to the norm. The point is that one could justify conformity if one reflected on the norm under ideal conditions (including having sufficient time, sufficient information, lack of bias, and so on). We also put aside the issue of *how many* members of a group have to conform for the norm to exist. We simply assume "almost all" and leave "almost" undefined.

[87] A situation is Pareto optimal when, and only when, it is not possible to improve the well-being of any one person without making others worse off.

[88] Since we allow data collected at one time to be indefinitely retained for future use, we need to introduce a temporal dimension into the definition of norm completeness. A more accurate statement would be: there is no significant tradeoff between privacy and competing goals at a given time that is not governed by at least one value-optimal informational norm existing at that time. We put aside the (important) complication that tradeoffs in the future may involve individuals who did not exist at the time the transaction was made.

First, it is plausible to assume that practice more or less approximates norm completeness for traditional, non-digital goods and services. Buyers and sellers have exchanged goods and services for centuries, and it is plausible to assume that, over the years, relevant value-optimal norms have evolved.[89] A critical concern that we address below is that rapid advances in technology have outstripped the relatively slow evolution of norms and created novel situations for which we lack relevant value-optimal informational norms.

Second, in assuming transactions are *governed* by norms, we are assuming that both visitors and businesses conform to the norms. This is certainly plausible for visitors since the norms in question implement values they hold. But what about businesses? Norm-conforming visitors look like easy targets for exploitation. What will keep profit-motive-driven businesses from imposing norm-inconsistent terms in Notices they know visitors do not read? We have given our answer in detail elsewhere.[90] Addressing this question is an essential part of the "toil" necessary to understand the role of norms in markets and cultures.

Finally, why take norm completeness as an ideal? Because, when it is true, every significant tradeoff is an acceptable one to which buyers give free and informed consent. We begin by explaining why tradeoffs governed by value-optimal norms are acceptable.

[89] The norm in now incorporated into the Implied Warranty of Merchantability, which is asserted in Uniform Commercial Code section 2-314(2)(c). For a fuller discussion, *see* JAMES OLDHAM, ENGLISH COMMON LAW IN THE AGE OF MANSFIELD (2004). The norm in now incorporated into the Implied Warranty of Merchantability, which is asserted in Uniform Commercial Code section 2-314(2)(c). For a fuller discussion, *see* Richard Warner & Robert H. Sloan, *Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access*, U. ILL. J.L. TECH. & POL'Y 101, 116–121 (2012).

[90] SLOAN AND WARNER, *supra* note 84.

B. Acceptable Tradeoffs

All informational norms—value-optimal and non-value-optimal alike—implement a tradeoff between privacy and competing concerns. They permit some information processing, and thus secure some of its benefits, but they protect privacy by allowing only certain processing. When the norm is value-optimal, the tradeoff it implements it is justified by visitors' values (with no alternative that better justified). The tradeoff is acceptable in this sense.

C. Why Consent is Informed

A visitor's consent is informed if the visitor can make a reasonable evaluation of the risks and benefits of disclosing information. Visitors easily meet this requirement as long as norm completeness holds. Norm-completeness ensures that every transaction is governed by appropriate value–optimal norms, and, as long as visitors know that their transactions are so governed, they know all they need to make a reasonable evaluation of the risks and benefits of disclosing information. They know all they need because uses of the visitor's information—both uses now and uses in the unpredictable future—will implement tradeoffs between privacy and competing goals that are not only entirely consistent with their values. Surely, that is enough to evaluate the risks and benefits.

Thus, when norm completeness holds, one may reject the specificity assumption. Informed consent does not require knowing in some detail "what information is captured, where it is sent, and how it is used."[91] Visitors just need to know that data collection and use will be consistent with relevant value-optimal norms. Some may object that this just substitutes one problem for another. The problem of finding a way to give visitors enough detailed information disappears, but another difficult problem takes its place: the problem of ensuring that

[91] Nissenbaum, *supra* note 7at 35. *See also infra* Section I, A.

appropriate value-optimal norms exist. Online data collection and analysis is one of many areas in which rapid advances in technology have outstripped the relatively slow evolution of norms and created novel situations for which we lack relevant value-optimal informational norms.

We do not disagree. Indeed, our point was precisely to replace the "knowledge of sufficient detail" problem with the problem of creating relevant value-optimal norms. We think this is where critical work needs to be done. We will return to this point shortly.

D. Why Consent Is Free

In our earlier discussion of free consent, we argued that even a highly constrained choice could be a free choice, but we left open the question of whether Vicky's constrained choice qualifies as free. Our answer is, "It depends."

It depends on whether the transaction is governed by relevant value-optimal informational norms. Assume it is. Then the norm-governed transaction give Vicky just want she wants and needs—a key time-saving means to pursue the plans and projects to which she is committed. She allots only a relatively small amount of time to purchasing books. She wants to purchase suitable books within that time and return to pursuing her other goals. She knows Amazon will process some range of personal information, and she wants an acceptable tradeoff between informational privacy and other relevant risks and benefits. The norm-governed transaction gives a *ready-made* value-optimal tradeoff. It is a highly efficient way for her to carry out her transaction with a minimum of attention or effort to privacy tradeoffs. Thus, as in the daycare and Cayman Islands examples, her constrained choice is the choice that fits in with

her other freely pursued plans and projects and is in this way an affirmative action in the pursuit of those plans.[92]

We conclude that, when buyers conform to value-optimal norms, buyers give free and informed consent to the norm-implemented trade-offs.

But what happens when a transaction is not governed by relevant value-optimal norms? Then there is no explanation of free and informed consent in terms of value-optimal norms, and, since we see no other effective mechanism for visitors to give free and informed consent, we conclude there is—as a practical matter—no effective way *at all* for visitors to give free and informed consent. Unfortunately this is precisely the situation website visitors face today. As we noted earlier, rapid advances in technology have created many situations for which we lack relevant value-optimal informational norms. The result is a radical failure of norm completeness. There are two ways this can and does happen: (1) relevant norms exist, but they are not value-optimal; or (2) relevant norms do not exist at all. We have discussed both cases in detail elsewhere.[93]

IV. A Key Task: Curing Failures of Norm Completeness

It is essential to develop a theory of norms and privacy,[94] and to find ways to generate appropriate norms when necessary. Our view happens to be that, with the notable exception of

[92] Elsewhere we argued that the third condition was not fulfilled but that its lack of fulfillment did not impugn the freedom of the choice. That argument is essentially the same as the argument we give her; we have simply chosen what we now regard as a better way to frame it. For the earlier argument, see SLOAN AND WARNER, *supra* note 84; Richard Warner & Robert H Sloan, *Behavioral Advertising: From One-Sided Chicken to Informational Norms*, VAND. J. ENT. & TECH. L. 15 (2012).

[93] Most fully in SLOAN AND WARNER, *supra* note 84. We offer a more technical discussion of some aspects of our theory in Warner and Sloan, *supra* note 92.

[94] See Meg McEvoy, *Commissioners Brill, Ohlhausen Discuss FTC Notice-Consent, Data Use Regulatory Models*, BLOOMBER BNA, PRIVACY LAW WATCH, March 13, 2013,

behavioral advertising, legal regulation is require to generate the needed norms, and we outline some norm-generating strategies in *Unauthorized Access: The Crisis in Online Security and Privacy*.[95] Our goal here, however, has just been to point out the "park" in which the work is to be done, not to argue for building a particular type of structure inside it.

http://www.bloomberglaw.com/document/X6M5N9GS000000?jcsearch=bna%2520A0D6X2D3B3#jcite (suggesting the need for data use norms).

[95] SLOAN AND WARNER, *supra* note 84.