THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XVIII STLR.ORG FALL 2016

ARTICLE

MEASURING PRIVACY: AN EMPIRICAL TEST USING CONTEXT TO EXPOSE CONFOUNDING VARIABLES †

Kirsten Martin and Helen Nissenbaum*

It is commonplace for those who support less restrictive privacy regulation on the collection and use of personal information to point out a paradox: in survey after survey, respondents express deep concern for privacy, oppose growing surveillance and data practices, and object to online tracking and behavioral advertising. Yet when confronted with actual choices involving the capture or exchange of information, few people demonstrate restraint: we sign up for frequent flyer and frequent buyer programs; we are carefree in our use of social networks and mobile apps; and we blithely hop from one website to the next, filling out forms, providing feedback, and contributing ratings. Privacy skeptics suggest that actions should be considered a truer indicator than words. Even if people are honest in their positive valuation of privacy in surveys, in action and behavior, they reveal even greater valuation of those benefits that might come at a privacy cost. In other words, people care about privacy, but not that much.

---

† The authors would like to thank the following for their helpful comments on this paper: Chris Hoofnagle, Mary Madden, Joel R. Reidenberg, Katie Shilton, and Joseph Turow. This material is based upon work supported by, in part, the National Science Foundation under Grant No. 1311823. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

This article may be cited as http://www.stlr.org/cite.cgi?volume=18&article=MartinNissenbaum.

* Respectively, Assistant Professor of Strategic Management and Public Policy at George Washington University School of Business; Professor of Media, Culture and Communication, and Computer Science at New York University, and Director of the Information Law Institute.

The inconsistencies between survey responses and observed behaviors that skeptics gleefully observe require a nuanced interpretation—one that we have offered through our studies. We argue that the disconnect between actions and survey findings is not because people do not care about privacy, but because individuals' actions are finely modulated to contextual variables. Questions in surveys that do not include such important contextual variables explicitly are highly ambiguous.

A more nuanced view of privacy is able to explain away a great deal of what skeptics claim is a divergence of behavior from stated preference and opinion. People care about and value privacy—privacy defined as respecting the appropriate norms of information flow for a given context. When respondents are given a chance to offer more fine-grained judgments about specific information-sharing situations, these judgments are quite nuanced. This is problematic since public policy relies on survey measurements of privacy concerns—such as Alan Westin's measurement of individuals as privacy 'pragmatists' or 'unconcerned'—to drive privacy regulations. Specifically, Westin's categories give credence to the regulation of privacy based by Fair Information Practice Principles (FIPPs), which relies heavily on assuring individuals notice and choice.

We examine two historically influential measurements of privacy that have shaped discussion about public views and sentiments as well as practices, regulations, and policies: (1) surveys of individuals' ratings of 'sensitive' information and (2) Alan Westin's privacy categorization of individuals as fundamentalists, pragmatists, and unconcerned.

In addition to replicating key components in these two survey streams, we used a factorial vignette survey to identify important contextual elements driving privacy expectations. A sample of 569 respondents rated how a series of vignettes, in which contextual elements of data recipient and data use had been systematically varied, met their privacy expectations.

We find, first, that how well sensitive information meets privacy expectations is highly dependent on these contextual elements. Second, Westin's privacy categories proved relatively unimportant in relation to contextual elements in privacy judgments. Even privacy 'unconcerned' respondents rated the vignettes as not meeting privacy expectations on average, and respondents across categories had a common vision of what constitutes a privacy violation.

This study has important implications for public policy and research. For public policy, these results suggest that relying on one dimension—sensitive information or Westin's privacy categorization of respondents—is limiting. In particular, focusing on differences in privacy expectations across consumers obscures the common vision of what is appropriate use of information for consumers. This paper has significant public policy implications for the reliance on consumer choice as a necessary approach to accommodate consumer variance: our results suggest consumers agree as to the inappropriate use of information. Our study has called privacy concepts into question by showing that 'sensitivity' of information and 'concern' about privacy are not stable in the face of confounding variables: privacy categories and sensitivity labels prove to be highly influenced by the context and use of the situation. Our work demonstrates the importance of teasing out confounding variables in these historically influential studies.

I. INTRODUCTION

Public opinion survey research has consistently played an important role in understanding privacy.[1] As novel technical systems and practices involving the collection, accrual, and use of information were introduced into American life, thought leaders sought to characterize the public's opinions about them. Dozens, if not hundreds of privacy surveys have been conducted—by academics, news media, polling companies—to ascertain: how people understand privacy; how much they value it; what they perceived as threatening to it; what they believed ought to be done; and more.[2] Accounts of public opinion and sentiment have been

---

1. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 43 (Univ. N.C. Press, 1995).

2. *Equifax Executive Summary 1991*, PRIVACYEXCHANGE, https://web.archive.org/web/20061002012321/http://www.privacyexchange.org/survey/surveys/eqfx.execsum.1991.html (last updated Oct. 2, 2006); Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SOC. SCI. RES. NETWORK (Sept. 29, 2009), http://ssrn.com/abstract=1478214 [http://www.webcitation.org/ 6lNW3afl6]; Mary Madden et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CTR. (Nov. 12, 2014),

important in various social domains: in public policy, they inform framers and advocates of regulation; in the commercial marketplace, they inform business and marketing strategy; in the sphere of technology, they drive design and development; and cutting across these, they inspire academic research.

It is commonplace for those who support less restrictive privacy regulation on the collection and use of personal information to point out a paradox: in survey after survey, respondents express deep concern for privacy, oppose growing surveillance and data practices, and object to online tracking and behavioral advertising. Yet when confronted with actual choices involving the capture or exchange of information, few people demonstrate restraint: we sign up for frequent flyer and frequent buyer programs; we are carefree in our use of social networks and mobile apps; and we blithely hop from one website to the next, filling out forms, providing feedback, and contributing ratings. Privacy skeptics suggest that actions should be considered a truer indicator than words. Even if people are honest in their positive valuation of privacy in surveys, in action and behavior, they reveal even greater valuation of those benefits that might come at a privacy cost. In other words, people care about privacy, but not that much.[3]

---

http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [http://www.webcitation.org/6lNTwVONg]; Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PEW RES. CTR. (Sept. 5, 2013), http://pewinternet.org/Reports/2013/Anonymity-online.aspx [http://www.webcitation.org/6lNWLKNXS]; JOSEPH TUROW ET AL., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION, (Annenberg Sch. for Commc'n. Univ. Pa., 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf [http://www.webcitation.org/6lNUQGKc5]; Chris Jay Hoofnagle & Nathan Good, *Web Privacy Census*, SOC. SCI. RES. NETWORK (June 1, 2012), http://ssrn.com/abstract=2460547 [http://www.webcitation.org/6lNWq9PzU]; Mika D. Ayenson et al., *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning*, SOC. SCI. RES. NETWORK (July 29, 2011), http://ssrn.com/abstract=1898390 [http://www.webcitation.org/6lNX5eQVF]; *Computers and the Internet*, GALLUP, http://www.gallup.com/poll/1591/Computers-Internet.aspx (last visited Sept. 4, 2015) [http://www.webcitation.org/6lNUiusLU]; John Fleming, *Millennials Most Trusting on Safety of Personal Information*, GALLUP, http://www.gallup.com/poll/183074/millennials-trusting-safety-personal-information.aspx (last visited Sept. 4, 2015) [http://www.webcitation.org/6lNV6hOtJ].

3. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (Stanford Univ. Press, 2010); Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*,

These arguments, as put forth by privacy skeptics, have been oddly resilient despite flaws that have been repeatedly identified: importantly, that people are largely unaware of the extent of data collection and have virtually no idea of what happens with information after it is collected or how these practices might affect them.[4] Furthermore, because opting out of activities that involve intensive data collection—for example, using credit cards and mobile phones—can be costly, the choices people are making in favor of such goods seemingly in a tradeoff against privacy are not—as skeptics would have it—free.[5]

Although these rebuttals are solid, one additional—and arguably even more telling—point is the reliance of privacy skeptics on conceptions of privacy that, in our view, do not map onto conceptions informing survey respondents. The inconsistencies between survey responses and observed behaviors that skeptics gleefully note require a nuanced interpretation—one that we have offered through our studies. Specifically, our work shows that frequently the disconnect between actions and survey findings is, "not because people do not care about privacy, as privacy skeptics have charged, but because our actions are finely modulated to the variables. Questions in surveys that do not fix these variables explicitly are, thus, highly ambiguous."[6]

If one holds that any release or sharing of information is incompatible with privacy, then everything people do on Facebook or even what they do in a physician's office conflicts with assertions they make on a survey about caring deeply about privacy and wanting stronger protection for it. But if one adopts a different definition of privacy (for which we have argued at length

---

First Int'l Forum on the Application and Management of Personal Electronic Information (Oct. 12–13 2009), https://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf [http://www.webcitation.org/6lNaru3xN]; Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 753 (2007).

4. Pedro Giovanni Leon et al., WHAT DO ONLINE BEHAVIORAL ADVERTISING PRIVACY DISCLOSURES COMMUNICATE TO USERS? 12 (Carnegie Mellon CyLab, 2012); Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MARKETING 210, 220 (2015); Turow et al., *supra* note 4, at 6.

5. NISSENBAUM, *supra* note 5, at 23–25.

6. *Id*. at 150.

elsewhere[7]), namely, as an appropriate flow of information, privacy can be compatible with quite a lot of sharing and disclosing. With this definition of privacy, only inappropriate sharing or disclosing conflicts with the survey findings. Thus, a nuanced view of privacy is able to explain away a great deal of what skeptics claim is a divergence of behavior from stated preference and opinion. People care about and value privacy—privacy defined as respecting the appropriate norms of information flow for a given context. When respondents are given a chance to offer more fine-grained judgments about specific information-sharing situations, these judgments are quite nuanced.[8]

Confronted with ambiguous or incompletely specified questions, however, respondents first must interpret and disambiguate, not necessarily uniformly. Our proposition is that respondents are effectively generating and responding to different versions of a given survey, so that aggregating overall responses as if they pertain to a single set of questions is likely to produce muddy results. Germane to the skeptics' paradox, we note that observed behaviors might, in fact, be compatible with some of the interpreted versions of survey responses as long as one believes, for example, that a patient sharing sensitive health information with a physician does not contradict that person's stated commitment to privacy.

Our studies aim to reveal systematic variation lurking beneath seemingly uniform responses in privacy surveys. To do so, we revisited two well-known privacy measurements that have shaped public discourse as well as policies and practices in their respective periods of greatest impact. We chose them both because of their centrality and influence and also because they are the products of highly regarded leaders in the field. One, Alan Westin's series of surveys, established that people (consumers) persistently fall into three categories in their valuations of privacy both online and offline: fundamentalists, pragmatists, and unconcerned.[9] The other attempts to measure persistent ratings of information along a scale of sensitivity; we use the Pew Foundation's survey as an example.[10]

---

7. *Id.* at 3; Kirsten Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy*, 137 J. OF BUS. ETHICS 551, 552 (2015).

8. *See, e.g.*, Judith S. Olson et al., *A Study of Preferences for Sharing and Privacy, in* CHI '05 EXTENDED ABSTRACTS ON HUM. FACTORS IN COMPUTING SYSTEMS 1985, 1987 (2005), dl.acm.org/citation.cfm?id=1057073 [http://www.webcitation.org/6liwBN8Ob].

9. Kim Bartel Sheehan, *Toward a Typology of Internet Users and Online Privacy Concerns*, 18 INFO. SOC'Y 21, 21 (2002).

10. Madden, *supra* note 4, at 7.

In addition to replicating key components in these two survey streams, our studies introduced further sets of questions that instantiated the original ones with more concrete variations. These additional questions were guided by the theory of contextual integrity, which asserts that several parameters are simultaneously crucial to determining people's judgments whether a given action does or does not violate privacy.[11] We operationalized this using factorial vignettes in which respondents were presented a series of 40 vignettes, systematically varying three factors: contextual actor (explained later), type of information, and information flow or use. 569 respondents rated the degree to which the vignette scenarios met their privacy expectations. The factorial vignette methodology (described in more detail below) allows researchers to identify a set of variables or factors and to discern the relative importance of each of the factors to a given target outcome. In our own studies we were able to dispute results claimed by the Pew and Westin studies by revealing systematic variation within the seemingly uniform patterns they had claimed. Our results were striking, revealing that:

1. The relative importance of types of sensitive information, identified in the Pew study, on meeting privacy expectations is highly dependent on the contextual factors—such as actors receiving the information as well as uses of information. In fact, how the information is used is more important to meeting/violating privacy expectations than the type and sensitivity level of given information.

2. Westin's privacy categories were not an important factor in judging privacy violations of different scenarios. Even privacy unconcerned respondents rated the vignettes to not meet privacy expectations on average. Respondents across categories had a common vision of what constitutes a privacy violation.

This study has important implications for research and public policy. For public policy, these results suggest that relying on one dimension—sensitive information, privacy categorization of respondent—is limiting. In particular, focusing on differences in privacy expectations across consumers obscures the common vision of what is appropriate use of information for consumers. Our study has called privacy concepts into question by showing 'sensitivity' of information and 'concern' about privacy are not stable in the face of confounding variables: privacy categories and sensitive labels prove to be highly influenced by the context and use of the situation. For future surveys of privacy, this study exemplifies the importance of including confounding variables in the study of privacy. The context

11. NISSENBAUM, *supra* note 5, at 7.

of an information exchange—how the information is used and transmitted, the sender and receiver of the information—all impact the privacy expectations of individuals.

Before explaining the methodology and results in sections III and IV, some background is necessary. In section II, we describe both survey streams—on sensitive information and privacy personality categories. We also introduce key concepts of contextual integrity in order to account for methodological choices.

II. BACKGROUND

A. Sensitive Information

In scholarship as well as common parlance, information may be labeled sensitive if it is thought to deserve additional protection measures on the grounds that disclosing it renders the information subject vulnerable to harm. Studies have shown that sensitive information is viewed as riskier[12], raises consumer privacy concerns[13], and requires greater protection[14] as well as greater governmental oversight.[15] For example, health information can be used to discriminate based on afflictions; pregnancy status can be used to discriminate against women in employment or financial information can be used to commit fraud. The harm need not be easily measurable: information that could cause embarrassment or general unease with disclosure can also be deemed sensitive.[16]

As Professor Paul Ohm nicely summarizes, "Sensitive information is a show stopper."[17] Practices become restricted and regulations suddenly appear when information is deemed 'sensitive': health information, financial information, video rentals, driver's license information, genetic information, and education records are all covered by their own regulation (Table 1). In the courts, Ohm

---

12. Naresh K. Malhotra et al., *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model*, 15 INFO. SYSTEMS RES. 336, 341 (2004).

13. Andrew J. Rohm & George R. Milne, *Just What the Doctor Ordered: The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern*, 57 J. OF BUS. RES. 1000, 1000 (2004).

14. Amitai Etzioni, *A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational*, 80 BROOK. L. REV. 1263 (2015).

15. Howard Beales & Jeffrey A. Eisenach, *Putting Consumers First: A Functionality-Based Approach to Online Privacy*, SOC. SCI. RES. NETWORK (June. 1, 2012), http://ssrn.com/abstract=2211540.

16. M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011).

17. Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015).

notes that social security numbers, nude photographs, and information about sexual activity deemed sensitive are regularly excluded from otherwise public availability of respective court records.

While important, the term 'sensitive information' is normally assigned for a type of information within research and practice. For example, the designation 'sensitive' information in research may be based on the "objective hazards posed by information revelation."[18] And, the designation is not always consistent in research or practice. Email is 'not sensitive' in some cases[19] yet is 'sensitive' along with username, password, birthday, and social security number for others.[20] In practice, Ohm notes the Network Advertising Initiative (NAI) defines health information as sensitive in a manner that differs from the Digital Advertising Alliance (DAA) and both definitions diverge from how companies such as Facebook and Google operationalize health information[21] as shown in Table 1. As observed by Professor Amitai Etzioni, this stream of scholarship sees sensitivity as "denoted rather than defined"[22]: the sensitivity label is designated regardless of the use of the situation. Although for purposes of this project, we have finessed the definitional quagmire, we note setting objective standards for sensitivity, is an intractable challenge, as demonstrated in Privacy in Context[23] chapter 6, because, to this day, ambiguities in the term "sensitivity" remain largely unacknowledged and unresolved.

But talking of sensitivity as if it can be objectively attributed to, or knowable of particular types or categories of information misses the contingency of such attributions on context and time. If we accept the definition of sensitive information as information that when disclosed renders information subjects vulnerable to harm, it is clear that all information has the potential to be sensitive subject to the shifting conditions of its disclosure. This relationship is easily seen in dramatic instances such as social security number and

---

18. Leslie K. John et al., *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. CONSUMER RES. 858–873 (2011).

19. Kim Bartel Sheehan & Mariea Grubbs Hoy, *Dimensions of privacy concern among online consumers*, 19 J. PUB. POL'Y & MARKETING 62–73 (2000).

20. Yan Sun & Shambhu Upadhyaya, *Secure and privacy preserving data processing support for active authentication*, 17 INFO. SYS. FRONTIERS 1007–1015 (2015).

21. Ohm, *supra* note 19, at 1139.

22. Etzioni, *supra* note 16, at 1281.

23. NISSENBAUM, *supra* note 5, at 103–128.

membership in the communist party, as well as with seemingly mundane information such as a person's name or race.[24] When public policy and research treat 'sensitive' as an objective classification, they mask crucial interdependencies between the sensitivity of information, on the one hand, and relevant contextual factors, on the other. Our study sets out to open this long closed box.

Table 1: Sensitive Information See also Ohm [25]

Public Policy	Scholarship	Practice
• Health: Health Insurance Portability and Accountability Act, • Financial: Gramm-Leach-Bliley Act, • Video rentals: Video Privacy Protection Act , • Individual's photograph, SSN, medical/disability info: Driver's Privacy Protection Act. • Cable subscriptions: Cable Communications Policy Act, • Genetic information: Genetic Information Nondiscrimination Act (GINA),	• Malhotra et al[26] include medical and financial (sensitive) versus lifestyle characteristics and shopping/purchasing habits; • For John et al [27] food preferences are inherently less sensitive than information about sexual preferences which allows the authors to compare the disclosure of 'sensitive' versus 'benign' information types. • Also known as 'personal information' as in	• NAI defines it as "information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history" • DAA defines it as "pharmaceutical prescriptions, or medical records about a specific individual". • Facebook is not allowed to target ads based on "disability or medical condition (including physical or mental health)." Google defines it as "health or medical information".

24. *See* NISSENBAUM, *supra* note 5, at 124.
25. Ohm, *supra* note 19, at 1150–61.
26. Malhotra et al., *supra* note 14, at 336.
27. John et al., *supra* note 20, at 858–873.

• 'Personal' info about children (name, address, phone number, SSN): Children's Online Privacy Protection Act, • Education Records: Family Educational Rights and Privacy Act.	Acquisti and Gross[28], Norberg et al[29].	

B. Westin's Categories: Privacy Pragmatists

Alan Westin's vast contribution to privacy in research and public policy cannot be overstated, including many of his accounts of privacy in terms of human freedom and autonomy.[30] In addition to his philosophical conceptions of privacy, Westin, in conjunction with Harris-Equifax and other corporate sponsors[31], conducted a series of widely-used surveys that have formed the basis for how we regulate and measure privacy in the United States. In his later work, Westin introduced three classes of individuals (if you will) in relation to privacy—fundamentalists, unconcerned, and pragmatists—derived from answers to three questions about privacy concerns (described below). Depending on how an individual answered these three questions, they were designated fundamentalist, unconcerned, or pragmatic.

Westin's categories have remained popular despite effective critical scrutiny, for example, by Professor Chris Hoofnagle and Professor Jennifer Urban, showing flaws in underlying assumptions

---

28. Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, 4258 LECTURE NOTES COMPUTER SCI. 36, 36–58 (2006).

29. Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100 (2007).

30. Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES 431 (2003).

31. PONNURANGAM KUMARAGURU & LORRIE FAITH CRANOR, PRIVACY INDEXES: A SURVEY OF WESTIN'S STUDIES 3 (Inst. for Software Research Int'l. 2005).

and Westin's methodology for assigning individuals to categories.[32] Historically, Westin's categories give credence to the regulation of privacy based by FIPPs, which relies heavily on assuring individuals notice and choice. Westin himself explicitly noted to Congress that fundamentalists are outliers and policy should be directed toward privacy pragmatists.[33] Since the pragmatists are most willing to 'trade' privacy off against other goods, this mainstream has the most to gain from the use of FIPPs, as it allows individuals to choose.[34] Scholarship demonstrating problems with overreliance on FIPPs as the primary mechanism governing privacy[35] has not significantly diminished the commitment in academia both to Westin's categories and informed choice as a backbone for the regulation of general information practices.[36]

For research and public policy, Westin's taxonomy of privacy dispositions has been problematic, in our view, on two counts. First, if differences of opinion devolve to dispositional differences (rather than, say, normative differences) companies and regulators are given license to make individual choices the nexus of regulation, thus lightening the burden on firms or lawmakers to making substantive commitments to privacy rights. The Network Advertising Initiative, for example, justifies its policies and practices with reference to Westin's categories, arguing that most individuals are willing to trade privacy for other goods.[37] Similarly, software companies reason that,

---

32. Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261 (2014).

33. *What Consumers Have To Say About Information Privacy: Hearing before the Subcomm. on Com., Trade, and Consumer Protection of the H. Comm. on Energy and Com.*, 107th Cong. 17–22 (2001) (testimony of Alan K. Westin, Professor Emeritus, Columbia University) [hereinafter *Hearing*].

34. DEP'T OF HOMELAND SEC., No. 2008-01, PRIVACY POLICY GUIDANCE MEMORANDUM (2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf; Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*. 6.3 I/S: J. L. & POL'Y FOR INFO. SOC'Y, 425, 443 (2011).

35. Barocas & Nissenbaum, *supra* note 5; Kirsten Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, 18 FIRST MONDAY (2013); Fred H. Cate, *The Limits of Notice and Choice*, 8 IEEE SECURITY & PRIVACY 59 (2010).

36. *E.g.*, H. Jeff Smith et al., *Information Privacy: Measuring Individuals' Concerns About Organizational Practices*, 20 MIS Q. 167 (1996).

37. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, 29–30 (2010), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

"privacy means different things to different consumers, and research has shown that there is a wide range of privacy sensitivities among individuals."[38] Accordingly, regulating privacy in the United States, has focused mostly on enabling and implementing consumer choice relating to given practices and very little on the substantive virtues of these practices themselves.

Second, Westin's choice of terms—privacy pragmatist or privacy unconcerned—is used to support the (incorrect) notion that some individuals are willing to give up all privacy interests in order to receive free services or discounts or targeted advertising. Such an assumption gives firms license to claim that disclosure of information is dispositive of an 'anything goes' approach to respecting privacy.[39] For example, Westin's privacy pragmatists and unconcerned supposedly explain why individuals disclose information on PatientsLikeMe website—where they are assumed to have no privacy expectations.[40] While the first implication supports focusing on 'consumer choice' as a necessary mechanism to appease supposedly 'divergent' interests, the second implication allows firms to claim that consumers have no interest in how information is subsequently used and consumers 'give up' or 'trade' privacy rights when disclosing information.

Table 2: Westin and Privacy Categories

Public Policy	Academia	Practice
● Westin testified before congress for privacy fundamentalist to be considered outliers and	● Sheehan et al [45]	● In advocating consumer choice, firms maintain that privacy means

38. *Understanding Consumer Attitudes About Privacy: Hearing Before the Subcomm. on Com., Manufacturing, and Trade of the H. Comm. on Energy and Com.*, 112th Cong. 30 (2011) [hereinafter *112th Hearing*] (statement of Michael Hintze, Associate General Counsel, Microsoft) (alternatively testimony by Alessandro Acquisti is an exception as he specifically states (in reference to Westin's oft-cited study), "In reality, however, certain practice met the unambiguous disapproval of a vast majority of U.S. consumers" and goes on to name them in studies by Tsai et al. (2009; 2011) and Turow).

39. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 152–153 (2004).

40. Thomas Goetz, *Practicing Patients*, N.Y. TIMES MAG., Mar. 23, 2008, at MM32.

45. Sheehan, *supra* note 11; Steven Bellman et al., *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, 20 INFO. SOC'Y 313 (2004).

policy to be directed toward 'pragmatists'.[41] ● Influence of Westin's studies categorizing consumers on FTC and protecting privacy.[42] See Hoofnagle response to FTC report.[43] ● DHS report links Westin's approach to FIPS with the	● Smith et al [46] ● Hui et al [47] ● Angst and Agarwal [48] ● Buchanan et al [49]	different things to different people [50] ●NAI before the FTC and congress uses Westin's surveys to explain that individuals are inconsistent in their concern for privacy.[51]

41. *Hearing*, *supra* note 35.

42. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

43. Letter from Chris Jay Hoofnagle to the FTC, Comments on A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change," (FEB. 18, 2011), https://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00347-57879.pdf [http://www.webcitation.org/6lPbyQVhe].

46. Smith et al., *supra* note 38.

47. Kai-Lung Hui et al., *The Value of Privacy Assurance: An Exploratory Field Experiment*, 31 MIS Q. 19 (2007).

48. Corey M Angst & Ritu Agarwal, *Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual persuasion*, 33 MIS Q. 339 (2009).

49. Tom Buchanan et al., *Development of Measures of Online Privacy Concern and Protection for Use on the Internet*, 58 J. AM. SOC'Y FOR INFO. SCI. AND TECH. 157 (2007).

50. *112th Hearing*, *supra* note 40.

51. The NAI provides an illustration of the problem with broad generalizations based on abstract privacy questions. The NAI maintained that the majority (55%) of consumers approve of browsing data to be used for ads with 'protections' based on the Harris/Westin surveys. *Behavioral Advertising: Industry Practices and Consumers' Expectations: Joint Hearing Before the Subcomm. on Com., Trade, and Consumer Protection and the Subcomm. on Com., Technology, and the Internet of the H. Comm. on Energy and Com.*, 111th Cong. 98–114 (2009) (statement of Charles Curran, Executive Director, Network Advertising Initiative). However, the actual survey asked "how comfortable are you when those websites [google, Yahoo!] use information about your online activity to tailor advertisements or content to your hobbies and interests" and 59% said they were not comfortable. When the question was modified to add that the website promised not to give the data to anyone else, 55% were comfortable (the number reported by NAI). ALLEN WESTIN, HOW ONLINE USERS FEEL ABOUT BEHAVIORAL MARKETING AND HOW ADOPTION OF PRIVACY AND SECURITY POLICIES COULD AFFECT THEIR FEELINGS 3–4 (2008), https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00052/544506-00052.pdf.

idea of informed consent for privacy and that individuals have different privacy preferences.[44]		● Explanations in the popular press include references to consumers not caring about or remaining unconcerned about privacy (e.g., Goetz, 2008).

C. Privacy as Contextual Integrity

According to the theory of contextual integrity protecting privacy means ensuring that personal information flows appropriately; it does not mean that no information flows, or that information flows only if the information subject allows.[52] Whether flow is appropriate depends on whether it conforms to legitimate, contextual informational norms. These norms prescribe information flows in terms of three parameters—actors (sender, subject, recipient), information types, and transmission principles. They are shaped by entrenched informational practices and contextual ontologies and informed by contextual goals and purposes. This means that when confronted with particular information flows, we judge them as respecting or violating privacy according to whether—in the first approximation—they conform to expectations of flow within a given context. When this is the case, we can say that contextual integrity has been preserved. When this is not the case, frequently when novel technologies are introduced that disrupt entrenched flows, the prima facie case exists for concluding that contextual integrity has been violated and privacy infringed. These charges can be rebutted if it can be shown that new patterns of flow are as good, if not better, than entrenched flows at promoting contextual ends and purposes (among other things). For example, a physician sharing patient health information with a third party, historically, has been considered a privacy violation but is sanctioned if the information in question is about a sexually transmitted disease and the third party is a public health authority.

One immediate consequence of defining informational privacy as contextual integrity is the sharp difference it reveals between

---

44. MacCarthy, *supra* note 36; DEP'T OF HOMELAND SEC., *supra* note 36.

52. NISSENBAUM, *supra* note 5; Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32 (2011); Helen Nissenbaum, *Respecting Context to Protect Privacy: Why Meaning Matters*, 22 SCI. AND ENGINEERING ETHICS 1 (2015).

"giving up" privacy and giving up information. As noted above, so frequently one hears privacy skeptics cite information–sharing practices as evidence that people do not value privacy as much as they say, or that they may value privacy but value other things much more. Privacy is not lost, traded off, given away, or violated simply because control over information is ceded or because information is shared or disclosed–only if ceded or disclosed inappropriately. That people are willing, even eager to disclose, release, and share information is quite compatible with placing a high value on privacy so long as such flows are appropriate. Giving up information, however much, is not the same as giving up privacy if the flow is appropriate. Posting news to a Facebook page, disclosing health information to a physician, or filing a tax return with the Internal Revenue Service does not amount to giving up privacy, only to giving up information. Although these information flows may be judged appropriate and not privacy violations or trade offs, they stand in contrast with other cases in which flows are deemed inappropriate either because they promote the advantage of others without serving contextual ends and values, or serve pressing, or dire purposes. At these times, we would recognize that privacy is violated or "given up," and not merely information.

The practical import of defining privacy as contextual integrity is to expose shortcomings in the design and interpretation of past surveys. A design that focuses on only one of the norm defining parameters without fixing the others, e.g., information type as medical diagnosis, would present ambiguous, or open-ended questions, requiring respondents to speculate on the status of the other parameters in order to answer. This would affect questions that ask respondents to judge the degree of sensitivity of information without specifying the context, actors, or principles of transmission. This would affect how the results of such surveys are interpreted and used and what they are presumed to teach us about expectations of privacy. Theories of privacy that consider the class of sensitive information as that which privacy protects are attuned to findings about degrees of sensitivity, for they would inform privacy policies regarding information on these grounds. Information high on the sensitivity scale deserves strong protection, strong constraints on flow–namely, collection, disclosure, and dissemination–in contrast with information low on the scale, which does not.[53]

According to contextual integrity, however, people's ratings for information types on a scale of sensitivity, while leaving

---

53. NISSENBAUM, *supra* note 5; Nissenbaum, *supra* note 54.

indeterminate the other parameters, are not predictive of their privacy judgments; the theory predicts these ratings will shift under variations of these parameters. As noted by Nissenbaum,

> [T]he framework of contextual integrity affirms intuitions that the capacities in which actors function are crucial to the moral legitimacy of certain flows of information. This holds true even when it appears that it does not—as when people remark that certain information is secret when they usually mean it is secret in relation to some actors, or constrained by a particular principle of transmission rather than absolutely.[54]

D. Research Questions

Our research sets out to test the robustness of the two common privacy metrics we have discussed above in light of contextual integrity: 1) placement within Westin's taxonomy, and 2) degree of information sensitivity. The former would suggest that privacy expectations are determined by levels of an individual's concern (unconcerned, pragmatist, fundamentalist); the latter that privacy expectations are determined by the sensitivity level of information (e.g. as found in Pew studies).[55] In contrast, contextual integrity would suggest that privacy expectations are systematically shaped by several factors simultaneously, including type of information, context, and how the information flows (or is used).[56]

Accordingly, we have explored:

---

54. NISSENBAUM, *supra* note 5 at 142.

55. PEW RESEARCH CENTER, *supra* note 4.

56. Measuring privacy expectations here differs slightly from measuring consumer expectations or customer satisfaction in the marketing literature. Valarie A Zeithaml et al., *The Nature And Determinants of Customer Expectations of Service*, 21 J. ACAD. MARKETING SCI. 1 (1993). Consumer expectations can be seen in one of four possible ways in scholarship: ideal, expected, deserved, and minimum tolerable. John A Miller, *Studying Satisfaction, Modifying Models, Eliciting Expectations, Posing Problems, And Making Meaningful Measurements*, CONCEPTUALIZATION AND MEASUREMENT OF CONSUMER SATISFACTION AND DISSATISFACTION 72–91 (Keith Hunt ed., 1976); Mary C. Gilly et. al., *The Expectation-Performance Comparison Process: An Investigation of Expectation Types*, INTERNATIONAL FARE IN CONSUMER SATISFACTION AND COMPLAINING BEHAVIOR 10–16 (Ralph L. Day and H. Keith Hunt eds., 1983). Importantly, this ambiguity about consumer expectations in marketing is around the prompt "What do you expect from [FIRM]?" and is open-ended. Here, the ambiguity could be around whether the expectations are ideal or merely adequate. Adequate privacy expectations could fall victim to the resignation found in privacy surveys—users become resigned to bad behavior. This interpretation would suggest the results may be conservative and respondents have stricter privacy expectations than measured here.

1. The importance of information sensitivity in relation to factors highlighted in contextual integrity.
2. How privacy judgments of sensitive information vary across different contexts.
3. How privacy expectations vary, if at all, in relation to information type, contextual actors, and information flows and uses.
4. The relationship between Westin's categories and privacy expectations.

Table 3: Privacy Measures with Public Policy and Research Implications

Privacy Defined By	Privacy Expectations Met If	Public Policy Implications	Tested Here
Sensitive Information	The information is not deemed 'sensitive'.	Focus on rules protecting types of information; e.g., video rentals, medical, children.	If 'sensitive' information is the dominant predictor of the degree the scenario meets privacy expectations.
Westin Privacy Categories for Consumers	Person is 'unconcerned' about privacy or, for privacy pragmatists, if the trade is attractive.	Consumers are assumed to have different dispositions or attitudes and firms should allow consumers to choose the privacy practices in the open market. No common understanding of privacy violations or expectations.	If Westin's categories are important predictor of the privacy rating of the scenario. We would expect Westin's category to be significant and important in determining privacy expectations.
Privacy as Contextual Integrity	Practices conform to rules of context or flow: Information type, contextual actor, and	Practices that respect contextual integrity could be the commonly accepted practices which would constitute the minimum standard for firms to manage privacy.[57]	The vignette methodology allows for multiple factors to be systematically manipulated to test how the factors work together to impact privacy expectation. We would expect the importance of information type to be

57. FED. TRADE COMM'N, *supra* note 39, at viii.

	transmission principles.		moderated by the contextual actor and use of information. Further, we would expect common privacy expectations based on contextual factors rather than the respondent's general concern or attitude towards privacy.

III. RESEARCH METHODS

A. General Methods

We applied two survey methodologies. First, we utilized traditional survey methodology to capture respondent-level measures of (1) standard controls, (2) Westin's privacy categories, and (3) respondent judgments of information sensitivity. Second, in order to assess measurements of 'privacy concern' and degrees of concern over 'sensitivity of information' in context, we sought a methodology that would be able to detect covariation of several factors. We deployed the factorial vignette survey methodology,[58] which allowed us systematically to change multiple contextual factors simultaneously while relying on a simple judgment for the rating task, namely, the degree to which the scenario meets privacy expectations.

Factorial vignette surveys present respondents with randomly generated vignettes in which experimentally designed factors are systematically varied across the vignettes. Respondents rate from 10–60 vignettes (here, respondents rated 40 vignettes randomly created with replacement) and are given the same rating task for all vignettes. Vignettes have been used in surveys generally where a respondent would be given a single vignette and asked a series of survey questions about that vignette. Here, respondents are given the same rating task over a series of vignettes and later analysis will identify which factors influenced the judgment of respondents positively and negatively.

---

58. Guillermina Jasso, *Factorial Survey Methods for Studying Beliefs and Judgments*, 34 SOC. METHODS & RES. 334 (2006); Stephen L. Nock & Thomas M. Guterbock, *Survey Experiments*, *in* HANDBOOK OF SURV. RES. 837 (Peter V. Marsden & James D. Wright eds., 2010).

In this manner, the factorial vignette methodology was designed to examine the normative judgments of respondents. Normative judgments are notoriously difficult to examine as respondents may attempt to bias answers to appear more ethical, and respondents may have difficulty identifying and articulating the reasoning behind their judgments.[59] Respondents are balancing 4–6 factors in rating each vignette which allows the respondent to determine the relative importance of each factor, all else being equal, when making the normative judgment about meeting privacy expectations. The factorial vignette methodology is ideally suited to research, such as this, which seeks to investigate the relative importance of several contextual factors simultaneously to whether privacy expectations are or aren't met.

The respondents were asked the questions in the following order:

1. Standard Controls (age, gender, trust, etc.)
2. Westin's Privacy Pragmatist Categories
3. Sensitive Information Measures
4. Factorial Vignettes

We chose this order to minimize priming. Previous studies found that showing respondents the realistic vignettes depicting online tracking and use of information affects the respondents' later measurements of trust and privacy concern. By placing the vignettes last, we sought to avoid unduly affecting their placement in Westin's taxonomy and their judgments about 'sensitive' information.

B. Respondent-Level Measures

1. Standard Controls

We captured the respondents' knowledge of the Internet, frequency of purchases online, and computer programming experience to capture experience online. In addition, respondents' were asked control questions about their institutional trust in websites as well as two privacy measures (the respondents' belief that privacy is important and their privacy concern). The respondents were asked to rate on a scale from 'strongly disagree' to 'strongly agree' their opinion of the statement: "In general, I trust websites" for respondents' institutional trust online. The second

---

59. Jonathan Haidt, *The Moral Emotions*, *in* HANDBOOK OF AFFECTIVE SCI. 852 (Richard J. Davidson et al. eds., 2003); Chen-Bo Zhong, *The Ethical Dangers of Deliberative Decision Making*, 56 ADMIN. SCI. Q. 1, 3–4 (2011).

rating task asked for their agreement with the statement, "[i]n general, I believe privacy is important." This rating captured respondents' general privacy belief. See Table 4 for a summary of the control variables.

Table 4: General Privacy Controls

GENERAL CONTROL QUESTIONS: Degree respondent agrees with the following.		
Question	Values	Prompt
Privacy Concern	-100 to +100	*I am concerned that online companies are collecting too much personal information about me.*
Trust in Websites	-100 to +100	*In general, I trust websites.*
Privacy Important	-100 to +100	*In general, I believe privacy is important*

2. Westin's Privacy Pragmatist Categories

We replicated Westin's privacy pragmatist measurements using three questions to categorize individuals as privacy unconcerned, privacy fundamentalist, and privacy pragmatist from Westin's and Harris surveys[60] and as analyzed by researchers since.[61] Respondents were asked to rate the degree to which they agree or disagree with the following statements:

1. Consumers have lost all control over how personal information is collected and used by companies.
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

Westin's categorization is then calculated according to the following:[62]

- Privacy Fundamentalists: Agree/Strongly Agree with 1, Disagree/Strongly Disagree with 2 and 3.

60. PRIVACYEXCHANGE, *supra* note 4; Westin, *supra* note 32, at 107–108.

61. *See* KUMARAGURU & CRANOR, *supra* note 33, at 20.

62. *Id*. at 4–5.

- Privacy Unconcerned: Disagree/Strongly Disagree with 1, Agree/Strongly Agree with 2 and 3.
- Privacy Pragmatists: All others.

Therefore, a fundamentalist must agree (to some degree) that "Consumers have lost all control over how personal information is collected and used by companies" and disagree (to some degree) with both "Most businesses handle the personal information they collect about consumers in a proper and confidential way" and "Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today." Although our critique of Westin's taxonomy is narrowly honed, thoughtful commentaries raise other considerations with his methodology.[63]

3. Sensitive Information

We replicated the questions asked in the Pew Internet study[64] (N = 607); respondents were asked: "Please indicate how sensitive you consider the following information to be—even if some people and organizations already have access to it" (with a rating of very sensitive, somewhat sensitive, not too sensitive, not at all sensitive). We included the top and bottom five sensitive information types from Pew Research report.

Top 5 most 'sensitive':

- Your social security number
- State of your health and the medications you take
- Content of your phone conversations
- Content of your email messages
- Details of your physical location over a period of time, gathered from the GPS data from your cell phone

Bottom 5 least 'sensitive':

- Your religious and spiritual views
- Who your friends are and what they are like
- Your political views and the candidates you support
- The media you like
- Your basic purchasing habits—things like the foods and clothes and stores you prefer

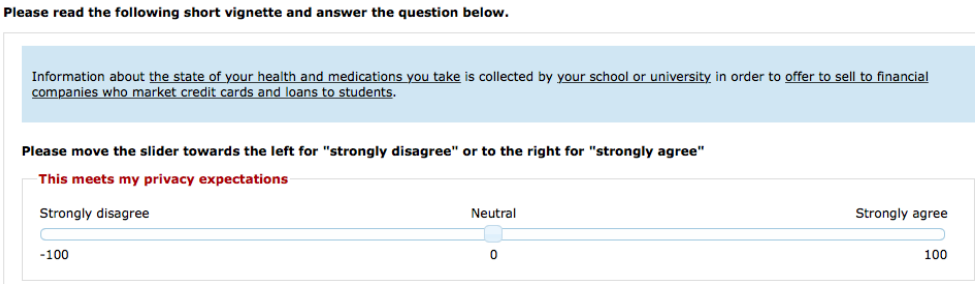
63. *See* Hoofnagle & Urban, *supra* note 34.

64. Madden, *supra* note 4, at 7.

4. Factorial Vignette Survey Design

Each respondent was presented with 40 vignettes in which factor levels were randomly varied by the researcher, in this case, through a survey instrument designed by the researchers. The survey instrument randomly selected with replacement the factor level for each vignette. Respondents were asked to rate the degree the vignette met their privacy expectations. See Image 1 for a sample vignette.

Image 1:

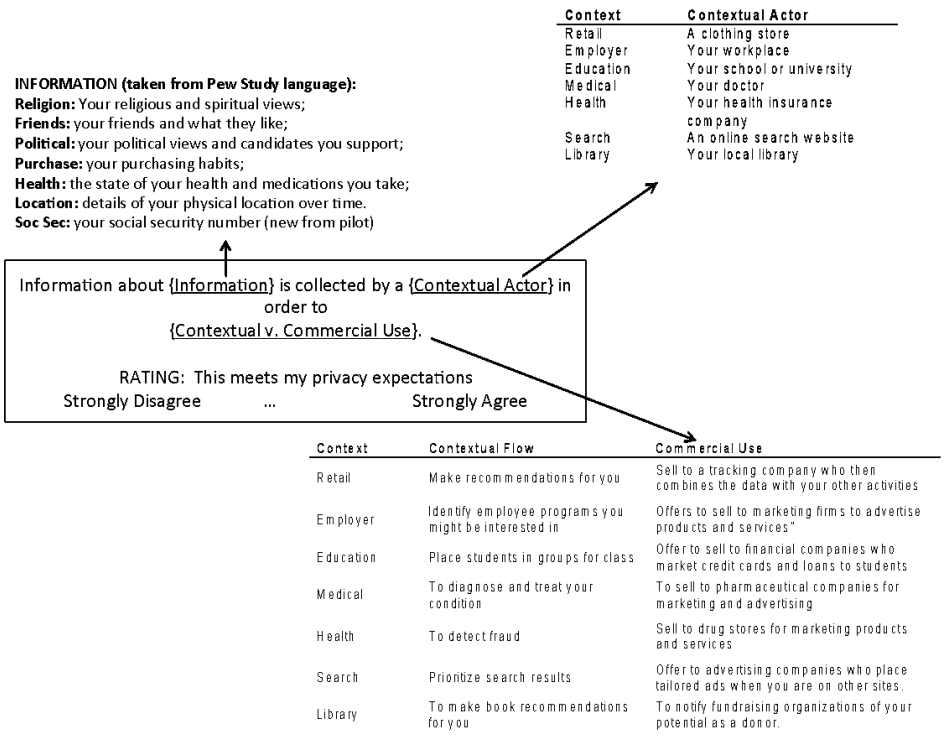


A full-blown operationalization of contextual integrity would have required five factor vignettes based on the parameters that contextual integrity postulates are critical to the definition of information privacy norms, specific to a given context, namely: sender, subject, recipient, information type, and transmission principle. Factorial vignette methodology suggests balancing the need for realism with the statistical validity of the analysis in choosing the number of factors and levels. [65] Accordingly, we took deliberate steps to simplify the task by holding certain variables constant, in order to limit the number of factors to three, and by significantly reducing the range and scope of those variables remaining. These choices increased the legibility to subjects of the vignette task while generating numbers per response that were sufficiently high for our analysis.

Thus, to contextualize information deemed sensitive in the Pew study we selected the following three factors, randomly varying them within the vignette, as shown in Figure 1:

Figure 1: Vignette Design

65. Jasso, *supra* note 60, at 335.



a. Information Types

Seven (7) types were included from the Pew study on sensitive information: religion, friends, political, purchase, health, location, and social security. We chose to exclude three information types—phone conversations, media preferences, and email content. In order to address respondent fatigue and increase statistical reliability, we decided to reduce the number of levels to seven. We chose these three because the vignettes including these three were highly implausible.

b. Contextual Actor (Recipient)

Seven (7) actors were selected based on their strong identification with seven distinctive contexts—retail, employer, education, medical, health, search, and library. With these, we sought to identify the influence of context on privacy expectations in relation to the information type variable.

c. Use/Flow

For each context, we included two alternative uses of the information. One, labeled contextual use, described options that subjects would understand as reinforcing the purposes and goals of respective contexts (per the theory of contextual integrity). For the latter, labeled commercial use, we included commercially driven flows and uses, given the prevalence of commercial secondary uses of information. [66]

5. Sample

The surveys were deployed through Amazon's Mechanical Turk where 569 respondents rated a total of 22,760 vignettes (40 for each respondent). Amazon Mechanical Turk (mTurk) offers a crowdsourcing platform for people who have a task to complete to be matched with people who wish to complete the task (Workers).[67] Although use of mTurk for survey deployment can be controversial,[68] studies have shown that mTurk Workers are more representative of the US population than the samples often used in social science research.[69] In a separate survey on privacy expectations for websites, the first author compared results from mTurk with results from a nationally representative sample from nationally representative survey from KnowledgeNetworks (GfK). The survey from the mTurk sample produces the same theoretical generalizations as the survey from the KnowledgeNetworks (GfK) survey, illustrating the ability to build generalizable theory from mTurk samples in online privacy studies.[70] See Table 5 for descriptive statistics of the sample.

Table 5: Summary of Sample Statistics

	Mean	S.D.

66. Martin, *supra* note 6, at 220; Kirsten Martin & Katie Shilton, *Why Experience Matters to Privacy: How Context-Based Experience Moderates Consumer Privacy Expectations for Mobile Applications*, 67 J. ASS'N FOR INFO. SCI. & TECH. 1, 1 (2015).

67. Gabriele Paolacci et al., *Running Experiments on Amazon Mechanical Turk*, 5 JUDGMENT & DECISION MAKING 411, 411–412 (2010).

68. Matthew Lease et al., *Mechanical Turk is Not Anonymous*, SOC. SCI. RES. NETWORK 1 (Mar. 6, 2013), http://papers.ssrn.com/abstract=2228728 [http://www.webcitation.org/6IJ9NIIIN]; Ross et al., *Who are the Crowdworkers?: Shifting Demographics in Mechanical Turk*, CHI '10 EXTENDED ABSTRACTS ON HUM. FACTORS IN COMPUTING SYSTEMS 2863, 2865 (2010), dl.acm.org/citation.cfm?id=1753873 [http://www.webcitation.org/6IJ88bMBU].

69. Paolacci, *supra* note 69, at 414.

70. Martin & Shilton, *supra* note 68, at 6–7.

PrivacyImportant	81.52	25.09
PrivacyConcern	51.83	39.05
TrustSites	-8.87	46.90
Coding	2.05	1.17
KnowInternet	2.93	0.95
Respondent R2	0.58	0.16
Average Rating	-40.31	31.26
Female	47%	

6. Analysis

The primary unit of analysis for the vignette survey is the scenario/vignette rather than the individual. Multi-level modeling is used as each individual (level 2) rates 40 vignettes (level 1) and independence of vignette ratings across individuals cannot be assumed. If I is the number of the respondents with level 2 individual variables and K is the number of vignettes answered with level 1 factor variables, the general equation is:

$$Y_{ij} = \beta_0 + \Sigma\beta_k V_{jk} + \Sigma\gamma_h R_{hi} + u_i + e_j$$

where Y_{ij} is the rating of vignette k by respondent i, V_{jk} is the k^{th} factor of vignette j, R_{hi} is the h^{th} characteristic of respondent i, β_0 is a constant term, β_k and γ_h are regression coefficients for *k* vignette factors and *h* respondent factors, u_i is a respondent-level residual (random effect), and e_j is a vignette-level residual. The model conceptualizes the ratings as a function of the contextual factors described in the vignette (ΣV_k) and the characteristics of the respondent (ΣR_h) as suggested above.

In addition, a respondent-specific equation[71] was developed by regressing the rating task on to the contextual factors for each respondent (N = 40). A new data set was formed for each survey with approximately 569 rows with a privacy equation for each respondent. The respondent-specific equation includes the respondent's intercept, the relative weight for each contextual factor, and a respondent-specific R2 as in equation below.

$$Y_i = \beta_i + \Sigma\beta_k V_k + e_i$$

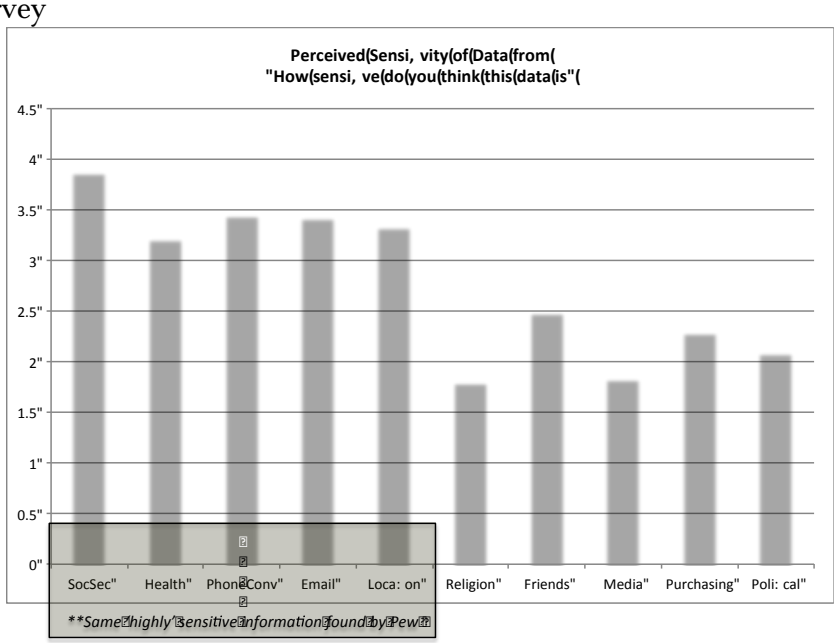
IV. RESULTS

71. Jasso, *supra* note 60, at 346-349.

A. Sensitive Information

In order to examine how respondents judge information deemed 'sensitive' within particular scenarios, the information was first measured with traditional survey methodology to replicate the findings in the Pew study before placing the information in context through the factorial vignette methodology. The traditional measurement of 'sensitive information' was analyzed through the use of the control questions around "How sensitive do you think the following data is". The average respondent ratings are shown in Figure 3. When asked in a traditional survey format, the results show the same ranking of 'sensitive' information as found in the Pew Study[72]: our respondents had the same top tier of sensitive information as the Pew respondents and the same bottom tier of sensitive information as shown in Figure 2.

Figure 2: Rating of 'Sensitive' Information from Traditional Survey



In order to understand how respondents judged information when placed in context, the vignette survey results were analyzed using multi-level analysis. The rating task—the degree to which the vignette met privacy expectations—was regressed onto the vignette factors as well as control variables. The results are in Table 3.

When judged in a scenario with the information, context, and use, respondents remain concerned with the type of information as all types have a negative impact on meeting privacy expectations

72. Madden, *supra* note 4, at 7.

when compared to just purchase information. However, the respondents also take into consideration the contexts of the vignettes; interestingly, situating the scenario in the retail context—where tracking user information is common—has the largest negative impact on meeting privacy expectations compared to other contexts and all else being equal (β =-14.64, $p < 0.001$). The commercial use of the information (rather than the contextual use of the information) dominates the judgments of respondents (β = -33.28, $p < 0.001$) as shown in Table 6. Out of the three highly 'sensitive' information types from the Pew Study, only social security is a significantly larger impact than other information types in violating privacy expectations.

Table 6: Results of Regressing Vignette Rating on Vignette and Control Factors

Relative Importance of Vignette and Control Factors		
	β	p
Information		
Friend Info	-9.80	0.00
Location Info	-14.21	0.00
Health Info	-14.78	0.00
Politics Info	-12.63	0.00
Religion Info	-11.69	0.00
Social Security Info	-38.38	0.00
(null = PurchaseInfo)		
Contextual Actor		
Education Context	-12.44	0.00
Employer Context	-10.78	0.00
Library Context	-2.33	0.04
Medical Context	-5.59	0.00
Health Insurance Context	-6.33	0.00
Retail Context	-14.64	0.00
(null = Search Context)		
Use		
Commercial Use	-33.28	0.00
(null= Contextual Use)		
Control Variables		
Age	-5.35	0.00
Gender	-1.85	0.42
Know Internet	1.15	0.37
Privacy Concern	-0.08	0.02
Trust Sites	0.13	0.00
Coding Experience	-1.14	0.28

Privacy is Important	-0.32	0.00
Westin's Privacy Unconcerned	7.29	0.05
Westin's Privacy Fundamentalist	-6.08	0.02
Constant	51.82	0.00
N (Vignettes)	22760	
N (Respondents)	569	
ICC	23.1%	

Placing Information in Context

In order to identify how respondents judge information across contextual actors, the dependent variable—meeting privacy expectations—was regressed on the interaction between information type and contextual actor. Figures 3a–e show how one type of information is judged differently depending on the context. The figures chart the impact of the information type on meeting privacy expectations when situated in different contexts, all else being equal. All interactions shown are significant ($p < 0.01$).

For example, purchase information is appropriate (has a positive impact on meeting privacy expectations) within the retail context but not appropriate within the health insurance context in Figure 6a. Similarly, political information is appropriate within search and a library but not appropriate within retail and medical; and friend information is positively received in retail, library, and education contexts yet negatively received in medical and health context across all flows and uses.

Even the most sensitive information is appropriate within context, including social security information and health information, which are rated 'most sensitive' by the general Pew study.

Figures 3a–e: Significantly Different ($p < 0.05$) Impact of Context on Importance of Information

Figure 3a: Religious Information

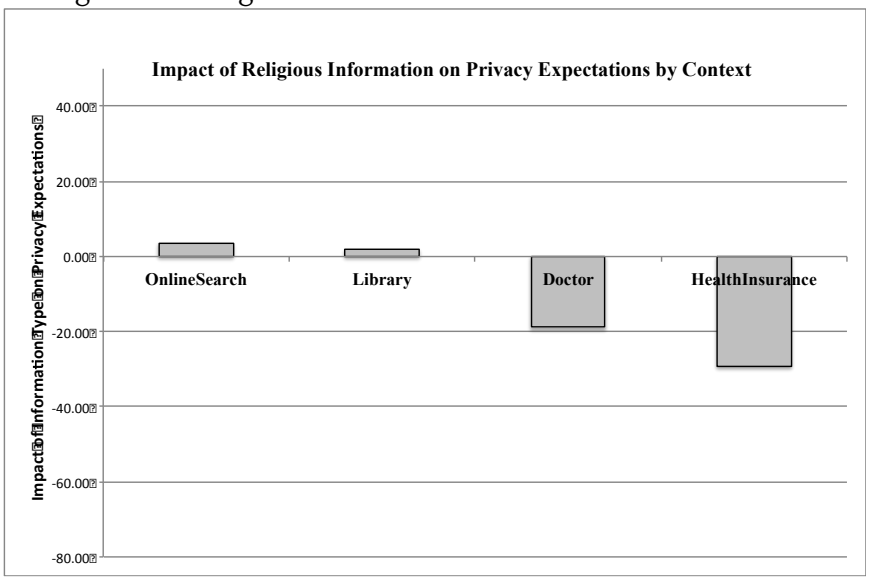


Figure 3b: Political Information

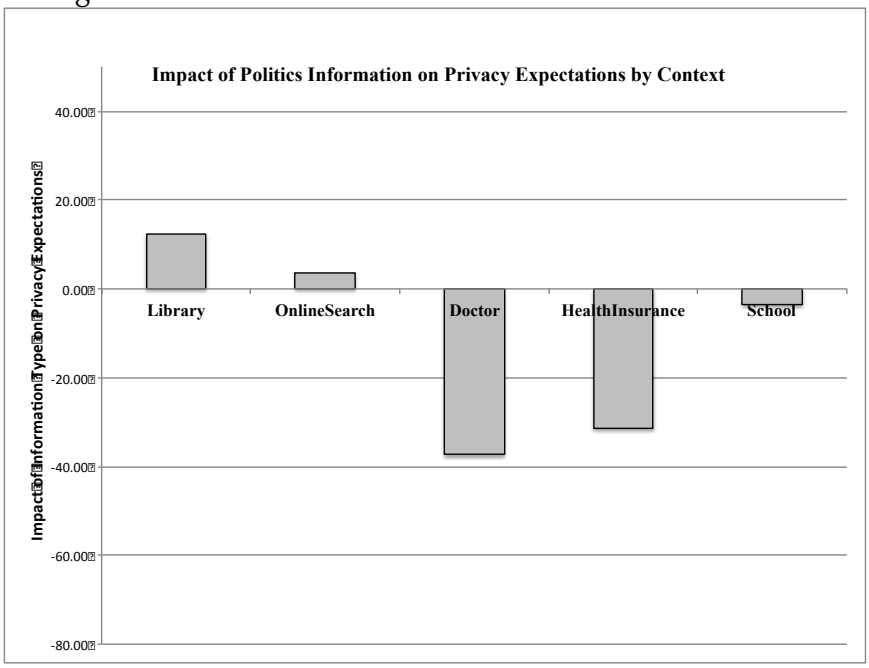


Figure 3c: Friend Information

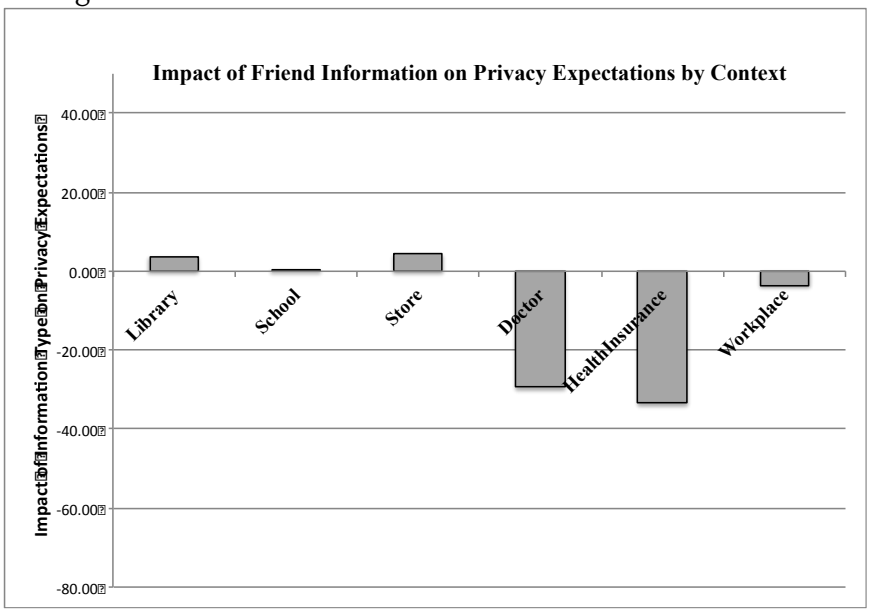


Figure 3d: Social Security Information

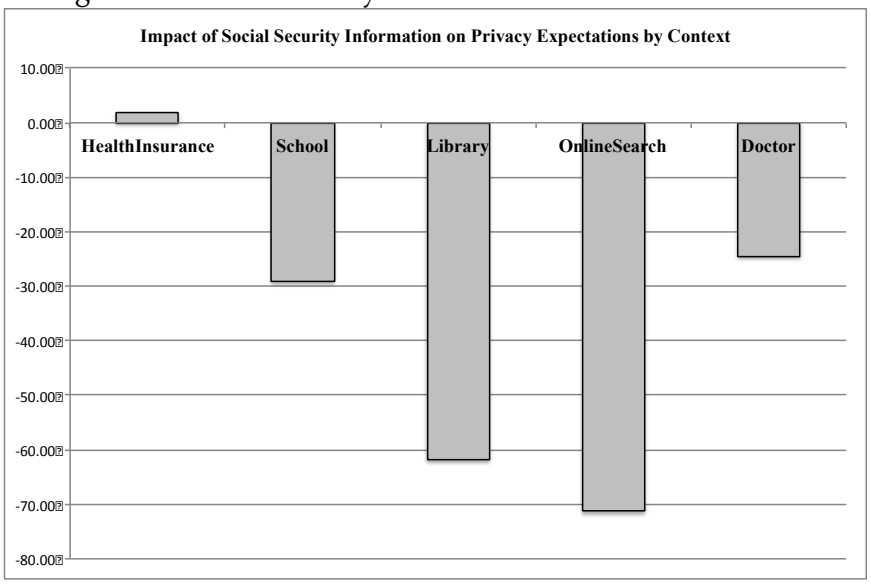
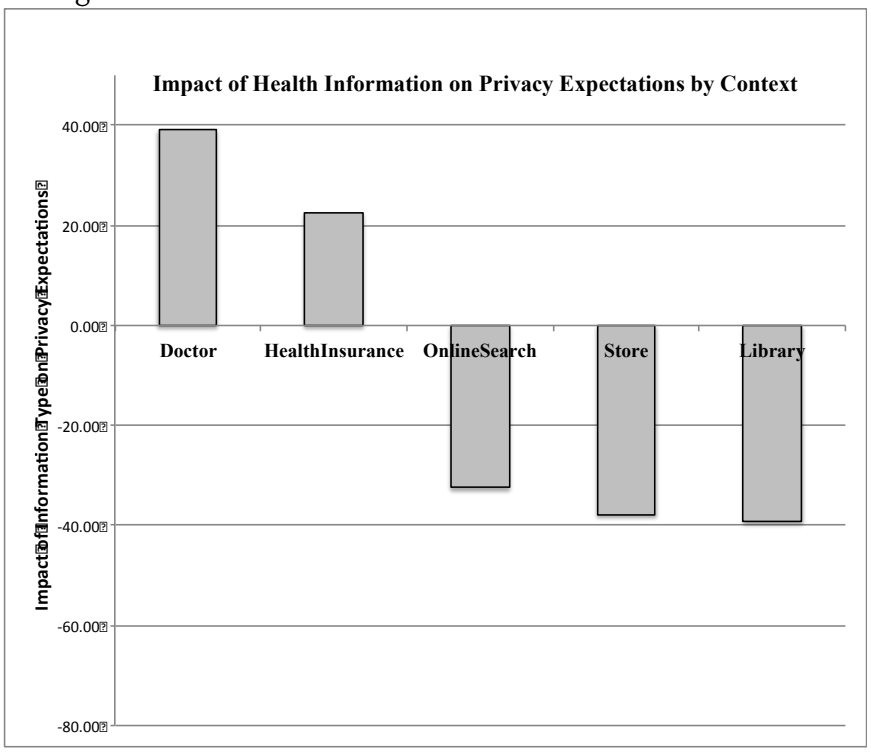


Figure 3e: Health Information



Finally, the 'sensitive' information is placed further in context by taking into consideration both the flow/use of information as well as the context. Figures 4a–f show the degree scenarios meet privacy expectations for contextual and commercial flows for a particular type of information across contexts. The graphs show the actual degree the scenario meets privacy expectations rather than the relative importance of the factors as in Figures 4a–f. For example, scenarios including friend information are only positively meeting privacy expectations within the education context and with contextual use as in Figure 4a. Scenarios including purchase information are only positively meeting privacy expectations within retail, library, and search contexts (again, with contextual use). All commercial uses of information negatively meet privacy expectations across all types of information and all contexts in Figures 4a–g.

Figures 4a–g illustrate the highly nuanced judgments respondents make in regards to the use of information as meeting or violating privacy expectations. Respondents are impacted by not only the type of information, but also by the contextual actor and the use of the information. If information could be objectively categorized as 'sensitive', the lines would be flat across contexts and

the lines would be conflated into one regardless of use. The peaks and valleys of the lines show the importance of the contextual actor. The gaps between the dotted (contextual use) and solid (commercial use) lines show the importance of flow/use of information. Any box around two points represents the instances are statistically identical.

Figures 4a–f: Degree Scenario Meets Privacy Expectations (Average Rating of Vignette): y = +100 means strongly agree that combination meets privacy expectations; y = -100 means strongly disagree.

Figure 4a: Friend Information by Context and Use

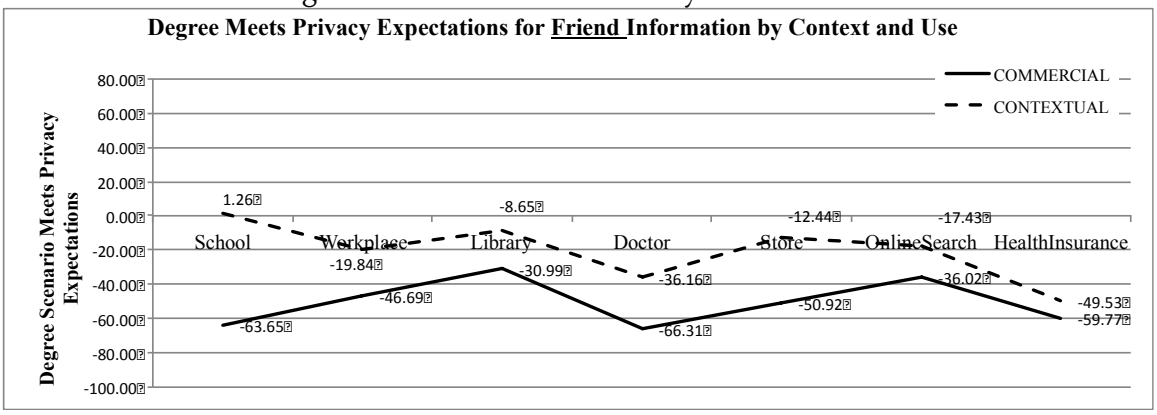


Figure 4b: Purchase Information by Context and Use

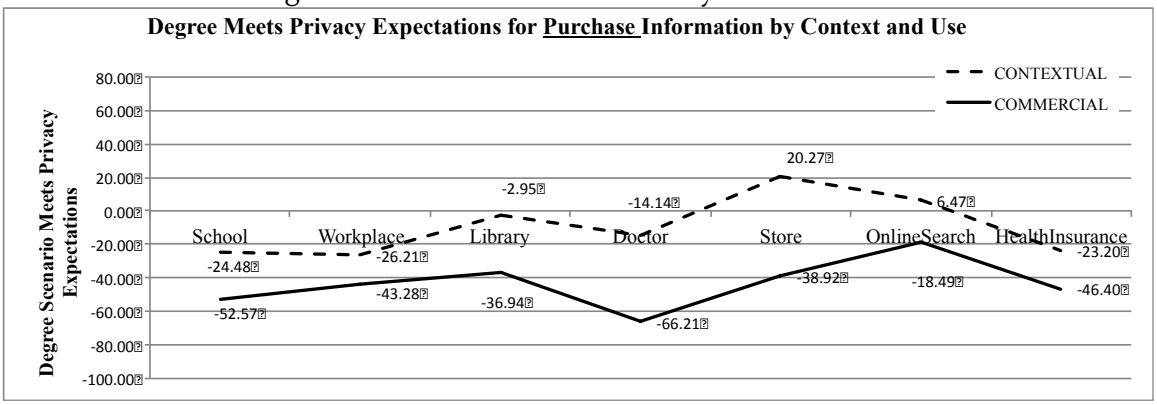


Figure 4c: Political Information by Context and Use

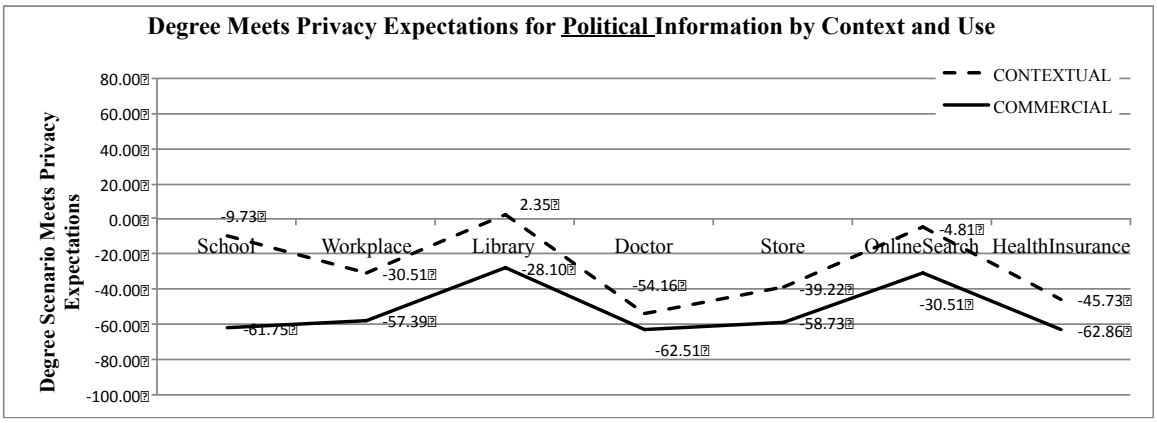


Figure 4d: Religious Information by Context and Use

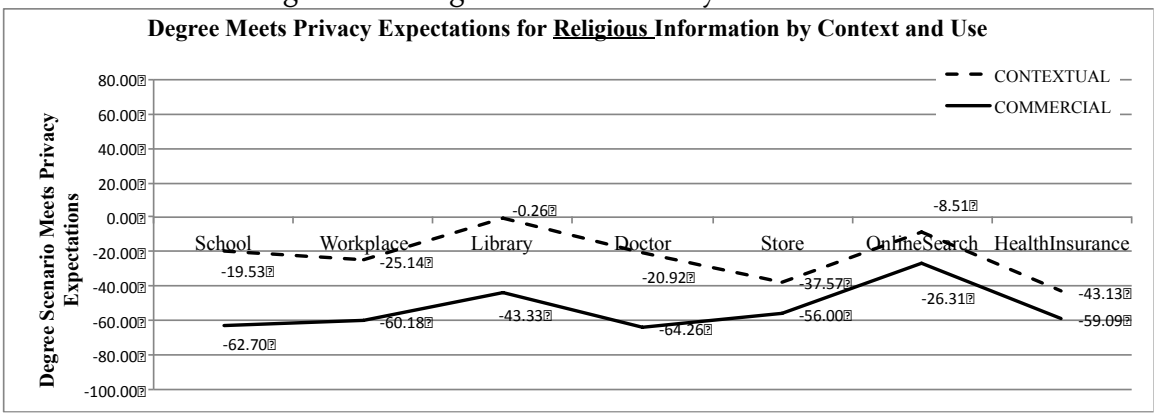


Figure 4e: Health Information by Context and Use

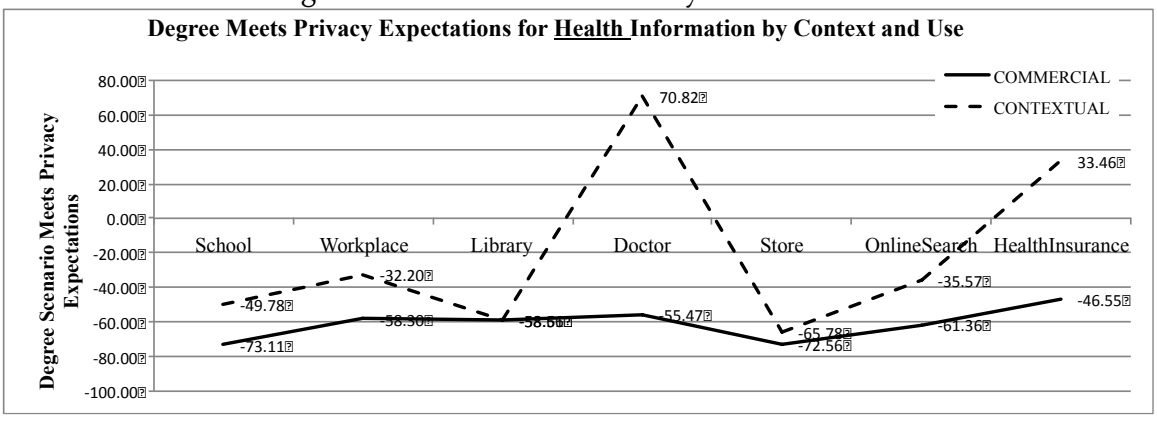


Figure 4f: Social Security Information by Context and Use

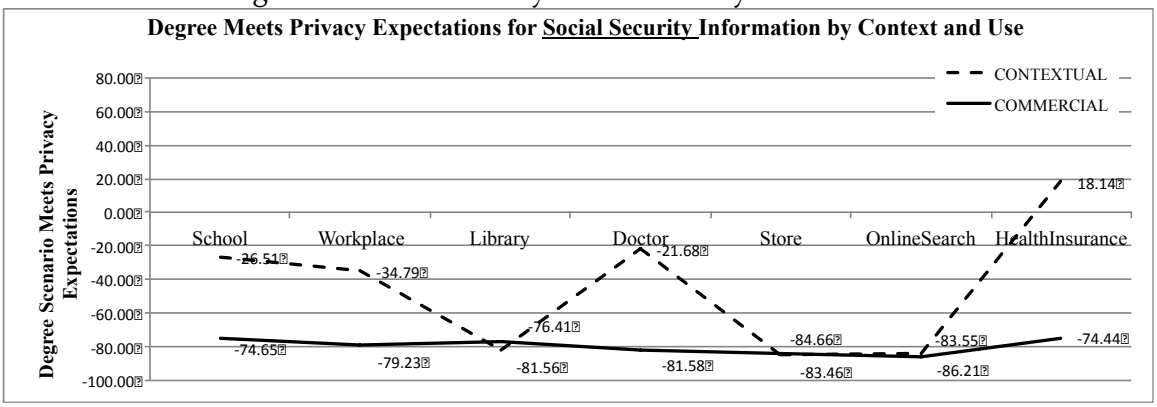
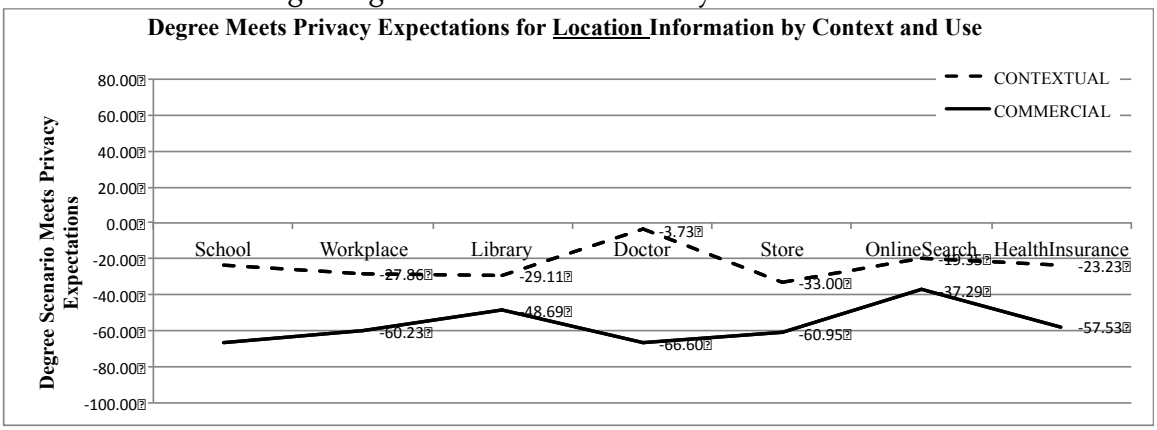


Figure 4g: Location Information by Context and Use



The most 'sensitive' information types based on Pew's initial study are shown in Figures 4f–g. Scenarios including health or social security information are consistently not meeting privacy expectations within commercial flows. However, both information types positively meet privacy expectations if used within particular contexts—medical and health respectively—and with appropriate use.

The results show that respondents are quite nuanced about judging the appropriateness of using their information when asked. The dotted lines in Figures 4a-f fluctuate across contexts and are even positive in meeting privacy expectations—even though respondents rate these information types as 'sensitive' when asked in an abstract traditional survey.

The results suggest that respondents may have a particular context and use in mind when they designate a type of information as sensitive. In particular, the commercial use of information across all contexts has a significant and important negative impact on meeting privacy expectations.

B. Role of Westin's Categories

The statistics of Westin's categorization into privacy pragmatists, fundamentalists, and unconcerned are summarized in Table 7. Respondents in this survey were categorized as privacy fundamentalists at a greater frequency than Westin's most recent survey in 2003. This disparity is primarily from respondents agreeing with first statement (consumers have lost all control over how personal information is collected and used by companies) to a greater degree (79% versus Westin's 69%) and disagreeing with the third statement (existing laws and organizational practices provide a reasonable level of protection for consumer privacy today) to a greater degree (65% versus Westin's 53% in 2003). Both contribute to a greater number of respondents within Westin's categorization of 'Fundamentalist'.

Table 7: Westin's Previous Survey Results (2003 and 1999) and This Survey

	Here	2003	1999
Pragmatists	42%	64%	54%
Unconcerned	13%	10%	22%
Fundamentalist	45%	26%	24%

In order to extend the understanding of Westin's privacy pragmatist categorization, the individual-level factors were included in the regression analysis in Table 6. Westin's categorization is a significant factor as shown in Table 3: Privacy Unconcerned positively impacts meeting privacy expectations ($\beta = 7.29$, $p = 0.05$) and Privacy Fundamentalist negatively impacts meeting privacy expectations ($\beta = -6.07$, $p = 0.02$) as compared to Privacy Pragmatists and when controlling for all other individual-control variables as in Table 6. The Westin categorization explains only 15% of the variance in the judgment about the vignette when compared with including only vignette factors.

More generally—and without controlling for any other individual factors—Privacy Fundamentalists do rate vignettes lower in not meeting privacy expectations (-50.59) compared to Privacy Pragmatists (-36.96) and Privacy Unconcerned (-16.02) as shown in Table 8. Importantly, all respondents across Westin's categorization find vignettes to not meet their privacy expectations on average since their average rating is negative. Even respondents categorized as 'unconcerned' by Westin's survey methodology judge vignettes as not meeting privacy expectations on average.

Table 8 includes the sample measurements by Westin's privacy categorization. Of significance, Westin's categorization may be more a factor of institutional trust as the difference between categories for respondents' 'trust-in-websites' is most pronounced in Table 8 with privacy unconcerned having a positive trust in websites generally (mean = 32.73) whereas privacy fundamentalists have a distrust in websites generally (mean = -30.99).

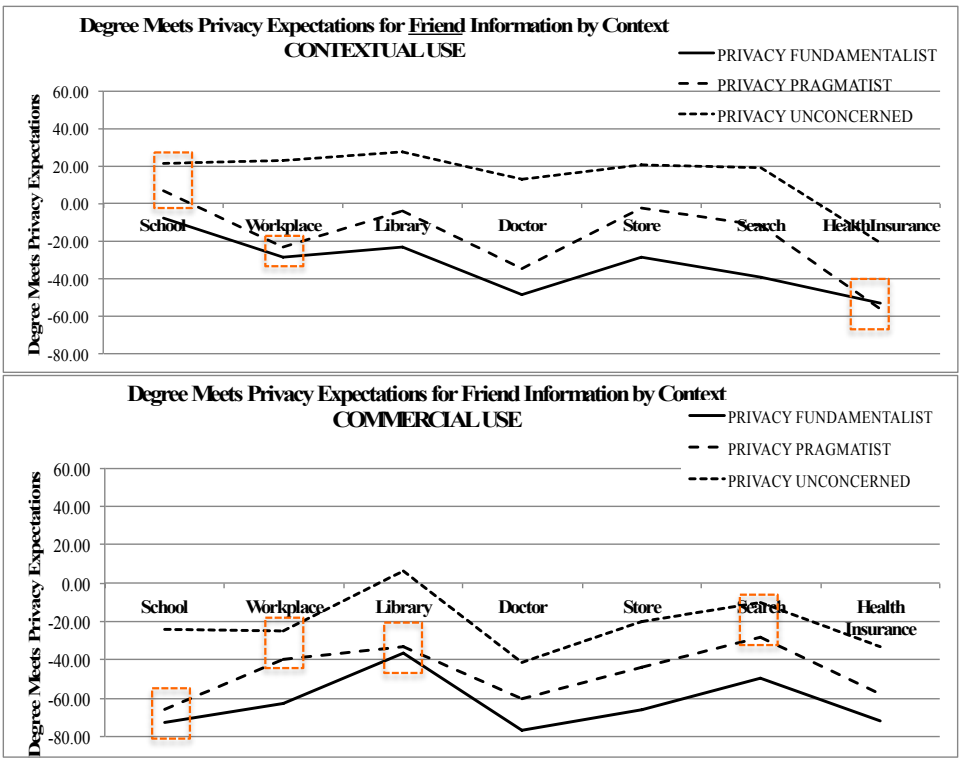
Table 8: Average Descriptive Statistics for Westin's Categories

	Vignette Rating Ave	Know Internet	Coding	Trust Sites	Privacy Import	Privacy Concern
Fundamentalists	-50.59	2.93	2.11	-30.99	87.05	65.75
Pragmatists	-36.96	2.90	2.07	1.67	81.19	49.23
Unconcerned	-16.02	3.01	1.83	32.73	63.75	12.83

Finally, we test the significance of Westin's categorization on privacy expectations of particular vignettes. Specifically, the degree to which each type of information meets privacy expectations within a particular context and with a particular use is compared across Westin's categories of respondents. The privacy expectation rating for each type of vignette was measured for subsets of the sample: only privacy fundamentalists (N = 255 respondents; 45% of respondents), privacy pragmatists (N = 239; 42%), and privacy unconcerned (N = 75; 13%). The results are in Figures 5a–g and show how little variation there is in privacy expectations across categories—particularly between privacy pragmatists and privacy fundamentalists. Both friend (Figure 5a) and health (Figure 5b) information are the exceptions with privacy unconcerned respondents rating vignettes to meet their privacy expectations to a greater extent and demonstrating less variation across contexts with the line being flatter.

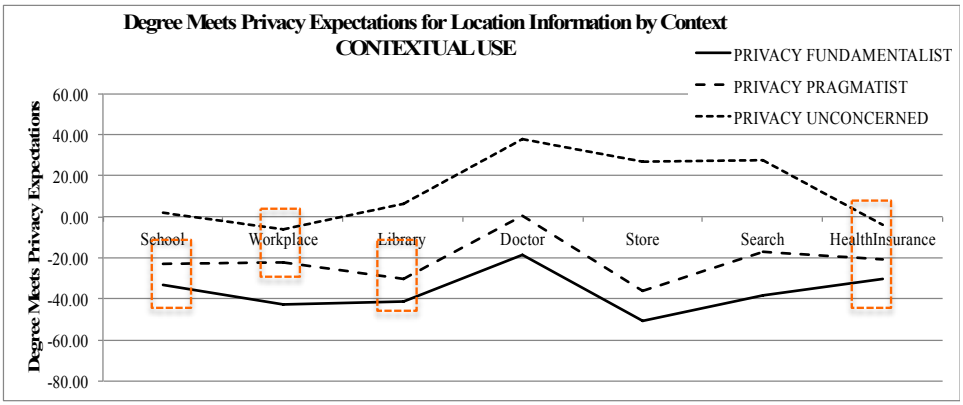
Boxes around the data points indicate no significant difference between Westin Respondent-types. Importantly, the difference between Westin's categories is not significant or not meaningfully important—particularly when compared to the significant and important difference of privacy expectations across different types of use in Figures 4a–g above.

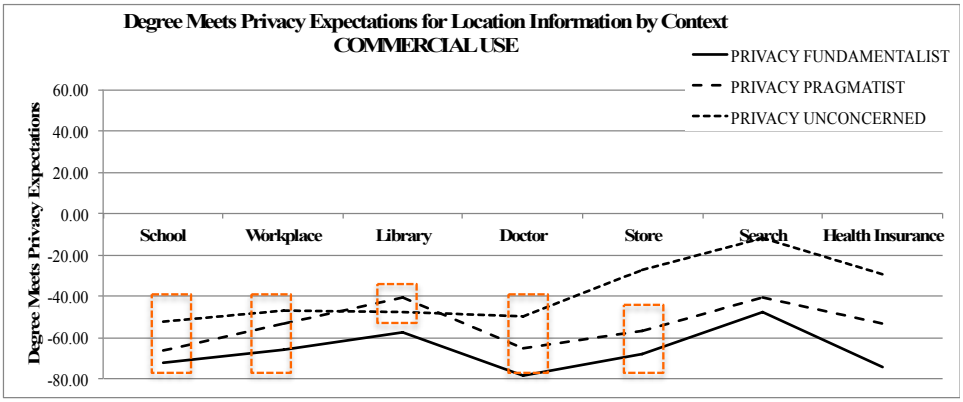
Figure 5a: Degree Friend Information Meets Privacy Expectations by Context, Use, and Westin Categorization



** Boxes around points signify statistically equivalent statistics.*

Figure 5b: Degree Location Information Meets Privacy Expectations by Context, Use, and Westin Categorization





** Boxes around points signify statistically equivalent statistics.*

V. SIGNIFICANCE OF FINDINGS

This study has shown the limited utility of Westin's categorization in differentiating privacy judgments. In fact, the use of the information—contextual v. commercial—explains the greatest amount of the variance of meeting privacy expectations across individuals. Interestingly, the commercial use of information consistently drove down privacy expectations, even for the retail context. The finding suggests that the commercial use of information is considered inappropriate even when the information has been willingly disclosed. These results have important implications for business and their use of information gathered across contexts.

For future surveys of privacy, this study reinforces the importance of how privacy is measured. Study designs should aim to disambiguate privacy rather than seek broad generalizations about consumers' privacy concerns. Past studies, including those that have been quite influential, have yielded cloudy and potentially

misleading results, i.e., misleading information about how people understand and value privacy. This study exemplifies the importance of including confounding variables in the study of privacy—the context of an information exchange, how the information is used and transmitted, and the sender and receiver of the information all impact the privacy expectations of individuals.

For public policy, this study suggests that relying on one dimension—sensitive information or not; privacy categorization of respondent—is limiting. Our study has called these concepts into question by showing 'sensitivity' of information and 'concern' about privacy are unstable in the face of confounding variables: privacy categories and sensitivity labels prove to be highly influenced by the context and use of the situation. In particular, focusing on differences in privacy expectations across consumers obscures the common vision of what is appropriate use of information for consumers. Claims that 'some people do not care about privacy' are shown to be unfounded in these results as even the respondents labeled 'privacy unconcerned' by Westin's categorization proved to have clear normative judgments about the inappropriate use of information. Follow-up work would need to identify the commonly accepted practices held to be inappropriate across consumers to aid in regulating privacy minimums.

A. Limitations

The factorial vignette survey methodology offers a path to add confounding variables for respondents to make privacy judgments. However, the methodology only captures the respondents' privacy judgments and not their actual behavior. Future work would need to extend this research to behavioral experiments to capture more than privacy expectations. In addition, a number of the factors in the privacy as contextual integrity theory were held constant, e.g., the sender of the information as well as the subject of the information. Future studies could focus on a different subset of contextual factors in order to measure privacy judgments. Finally, the sample was focused on U.S. respondents.

B. Sensitive Information

Type of information is significant, but not the most important factor in determining privacy expectations. Even placing information in a realistic scenario changes the degree to which respondents judge the information to be 'sensitive'. Placing 'sensitive' information in context matters. For example, health

information is positively judged within the medical context and negatively judged within the retail, search, and library contexts. On the other hand, religious affiliation is negatively judged within the health insurance context and positively judged within the library context. Information type is significant when understood in combination with the contextual actor receiving the information. Information type can positively impact meeting privacy expectations with one context while being judged a privacy violation in another context.

Even more important to violating privacy expectations was how the information was used or flowed. The results suggest less focus on how sensitive information is in general and more focus on the contextual norms of the firm and how the information is subsequently used or flows. Further, measurements of the sensitivity of information do not easily translate into privacy expectations in actual scenarios. The use/flow of information—specifically, the contextual use versus the commercial use of information—is the key driver of meeting privacy expectations and should be the focus of governing firm practices around information privacy.

For example, respondents might agree that information about sexually transmitted diseases is sensitive; might disagree that a physician can inform, parents without permission of the patient; but, might agree that the physician may inform public health authorities if mandated by law. Similarly, they may consider it offensive to their privacy if information they have placed low on the sensitivity scale is shared inappropriately. In our re-examination, we have demonstrated the ambiguity of unfinished questions by teasing out the sensitivity of people's responses to variations in relevant parameters. The primary aim of this work is to call into question what useful inferences can be drawn from judgments of sensitivity and to influence the design of future such surveys so they take into account all parameters required to define information norms. The relative importance of a type of information to meeting privacy expectations is highly dependent upon the contextual actor receiving the information, e.g, library, health insurance, retail store, etc.

C. Westin's Categories

The results suggest that Westin's categories of privacy fundamentalist, pragmatist, and unconcerned have limited application to consumers judging privacy scenarios. Consumers across the three categories had more in common than previously theorized as shown in Figures 6a–g where the respondents' privacy

judgments across information, contextual actor, and use were similar. Westin's categories impact privacy expectations slightly—however, even 'privacy unconcerned' respondents find the vignettes do not meet privacy expectations. Further, respondents across Westin's categories share similar or even identical privacy expectations. Differences in privacy expectations were explained by contextual factors rather than Westin's categories. Some of the variation in the privacy judgments was attributable to the differences in the individuals; however the majority of the variation could be ascertained from the scenarios, suggesting companies and regulators could identify commonly understood privacy violations. In fact, Westin's categorization may be a proxy for general institutional trust.

The perspective of contextual integrity on Westin's categories does not directly take up the findings that respondents fall into rough groupings based on answers to his questions; instead it calls into question the interpretation of these findings and their relevance to policy. As noted earlier, Westin's categorization of respondents in terms of persistent personality traits in their bearing to privacy has comfortably aligned with the position on privacy as a preference, which is respected when people are left to make their own privacy choices. Any substantive position on particular sets of constraints would disregard evident diversity in points of view. Our survey presents respondents with questions that insert ranges of values for the respective parameters contextual integrity asserts as fundamental to informational norms.

The results are striking, for even though we are able to replicate Westin's general groupings, we discover that these patterns are overridden by the impact of variable flows reflecting expected versus surprising flows. The figures illustrating the statistically identical privacy expectations across Westin's privacy categories show privacy expectations varied across contexts and uses of the information but varied little across types of respondents. It is possible to identify minimum standards of privacy that are shared by many users. Users do not have vastly different expectations of privacy within a particular context.

The results call into question any measurement of 'privacy unconcerned' and the consistent refrain that users do not care about privacy. The 'privacy unconcerned' (13% of the sample) still found the scenarios to be a privacy violation on average. The most significant difference across the Westin categories is the respondents' trust in websites generally (a measure of institutional trust), suggesting any differences across the categories could be a matter of trust rather than mere concern.

D. Privacy Paradox

As noted above, privacy skeptics point out that people's behaviors belie what they say in surveys and conclude that behavior is the truer measure of their valuation of privacy. We do not offer an alternative account of the inconsistency; instead, we show that many of the behaviors in question do not, in fact, contradict what people say in surveys. The results call into question the pervasiveness of the 'privacy paradox' mentioned above: where respondents express deep concern for privacy, oppose growing surveillance and data practices, and object to online tracking and behavioral advertising, yet continue to go online and (perhaps inadvertently) share information. The results here illustrate the limited meaning in abstract measures of privacy that form the basis for such a 'paradox': when respondents, who later disclose information and engage on social networking sites, are measured to be fundamentalists about privacy, the survey measurement may be flawed rather than the respondents.

This contradiction has been previously explained by noting that consumers frequently do not understand firm practices online or that consumers face difficulty in choosing privacy protective measures online.[73] Although we find these counter arguments convincing, our work supplements them with a further observation—that the assumed measurement of the privacy 'concerned' may be misleading and ineffective in explaining differences in privacy judgments. Where privacy skeptics place the onus on individuals in making better choices online, our findings suggest that firms would do better to focus on the manner in which consumer data is used if they want to meet users' privacy expectations.

---

73. James P. Nehf, *The FTC's Proposed Framework for Privacy Protection Online: A Move Toward Substantive Controls or Just More Notice and Choice?*, 37 WM MITCHELL L. REV. 1727, 1734 (2011).