

6-1-2014

Alan Westin's Privacy Homo Economicus

Chris Jay Hoofnagle
Berkeley Law

Jennifer M. Urban
Berkeley Law

Follow this and additional works at: <http://scholarship.law.berkeley.edu/facpubs>



Part of the [Law Commons](#)

Recommended Citation

Chris Jay Hoofnagle and Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 *Wake Forest L. Rev.* 261 (2014),
Available at: <http://scholarship.law.berkeley.edu/facpubs/2395>

This Article is brought to you for free and open access by Berkeley Law Scholarship Repository. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.

ALAN WESTIN'S PRIVACY *HOMO ECONOMICUS*

Chris Jay Hoofnagle*
Jennifer M. Urban**

INTRODUCTION

A regime of “notice and choice” largely governs U.S. Internet privacy law.¹ Companies, long encouraged by regulators, issue privacy policies² for consumers to read and act upon. In theory,

* Chris Jay Hoofnagle is a lecturer in residence at the University of California, Berkeley, School of Law, where he teaches computer crime law, privacy, Internet law, and a seminar on the Federal Trade Commission.

** Jennifer M. Urban is an Assistant Clinical Professor of Law and Director of the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley, School of Law. She teaches and researches in the fields of privacy, intellectual property, and information policy.

The authors thank Dr. Su Li, Dr. Joseph Turow, Jennifer King, Deirdre K. Mulligan, Tal Zarsky, Michael Birnhack, our Princeton Survey Research Associates colleagues, Larry Hugick and Margie Engle-Bauer, and Robert Barr for support in framing questions, analyzing data, and raising funds for this multiple-year effort. We thank each of these colleagues and participants in the Berkeley Center for Law and Technology Privacy Law Forums, the Santa Clara High Technology Law Journal's Mobile Revolutions symposium, the British Columbia Privacy and Security Conference, the Amsterdam Privacy Conference, the Brussels Computers, Privacy, and Data Protection Conference, and the Wake Forest Law Review 2013 Symposium for comments and critiques. We thank Chan Hee Chu for research assistance and the *Wake Forest Law Review* editing team. We also thank the financial supporters of our survey research, The Rose Foundation for Communities and the Environment, Nokia Corporation, and are grateful for additional funding from several *cy pres* funds. No funder reviewed any of our survey instruments or reports in advance of their posting or publication. In part, this Article collects and publishes survey results and analysis posted online in a series of Berkeley Consumer Privacy Survey reports, archived online at <http://www.law.berkeley.edu/privacysurvey.htm>. It includes some data first published in short form in Jennifer Urban et al., *Mobile Payments: Consumer Benefits & New Privacy Concerns*, EUR. FIN. REV. (Feb. 20, 2013), <http://www.europeanfinancialreview.com/?p=6301>.

1. ROBERT H. SLOAN & RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND SECURITY 79 (2014) (“The ‘notice’ is the presentation of terms, typically in a privacy policy or a terms-of-use agreement [on a website]; the ‘choice’ is an action, typically using the site or clicking on an ‘I agree’ button, which is interpreted as the acceptance of the terms.”).

2. Privacy policy adoption increased dramatically after the Federal Trade Commission encouraged companies to develop and post them online. See FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE

consumers read these notices and make decisions according to their overall preferences, including preferences about privacy, price, service offering, and other attributes.³ Privacy enforcement, in large part, addresses deceptions in these privacy policies rather than the fairness of their underlying terms.⁴

In recent years, notice and choice has come under growing and sustained criticism, including criticism from regulators and businesses, in light of evidence that it may be ineffective.⁵ Yet it remains the central feature of U.S. privacy law.

This Article contributes to the ongoing debate about notice and choice in two main ways. First, we consider the legacy of Professor Alan F. Westin, whose survey work greatly influenced the development of the notice-and-choice regime, and engage in sustained textual analysis, empirical testing, and critique of that work. Second, we report on original survey research exploring Americans' knowledge, preferences, and attitudes about a wide variety of data practices in online and mobile markets. This work both calls into question long-standing assumptions used by Westin and lends new insight into consumers' privacy knowledge and preferences.

The hegemony of the notice-and-choice regime is in no small part due to the prolific and influential work of Professor Westin, who passed away in 2013. Westin contributed substantially to information privacy theory and practice⁶ and is rightly considered a

ELECTRONIC MARKETPLACE 10 (2000) (noting a "significant increase" in the percentage of websites posting privacy policies in the year following a Federal Trade Commission report on the subject).

3. See 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) ("Under the FTC's self-regulatory principles, protecting consumer privacy is largely the responsibility of individuals who are expected to learn about the privacy practices of data collectors and take steps to minimize privacy risks.").

4. Mark E. Budnitz, *The FTC's Consumer Protection Program During the Miller Years: Lessons for Administrative Agency Structure and Operation*, 46 CATH. U. L. REV. 371, 396 (1997); G.S. Hans, Note, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 171 (2012).

5. There is a large amount of commentary to this effect. See, e.g., Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1880–82 (2013); Steve Lohr, *Redrawing the Route to Online Privacy*, N.Y. TIMES, Feb. 28, 2010, at BU4 ("There are essentially no defenders anymore of the pure notice-and-choice model," said Daniel J. Weitzner, a senior policy official at the National Telecommunications and Information Administration of the Commerce Department. "It's no longer adequate.").

6. Margalit Fox, *Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83*, N.Y. TIMES, Feb. 23, 2013, at D7 ("Mr. Westin was

father of contemporary privacy thought and policy. He wrote the seminal work *Privacy and Freedom*,⁷ perhaps the most important early contribution to information privacy law. In his academic work, Westin recognized privacy as a liberal value that all humans, and even animals, seek.⁸ His observations on this front were prescient. In 1967, he wrote in *Privacy and Freedom*: “The real need is to move from public awareness of the problem to a sensitive discussion of what can be done to protect privacy in an age when so many forces of science, technology, environment, and society press against it from all sides.”⁹ Westin believed that privacy was an important value, yet one that needed to accommodate other societal needs.¹⁰ He challenged policymakers to define privacy and to establish it as a concrete topic in political debates so that it could be invoked in a meaningful and bounded way.¹¹

Today, however, Westin's influence stems largely from the dozens of public-opinion poll surveys that he conducted along with his other research, which probed individuals' attitudes toward privacy and technology.¹² This survey research constitutes Westin's most famous work, and for decades, researchers, particularly in the business sector, have accepted its assumptions.¹³ Both industry actors and policymakers have relied on it and advocated its use.

Over the years, Westin's survey work lent strong support to the notice-and-choice approach; this is a predominant feature of his influence on policy. It proceeds from a highly influential segmentation model that divides consumers into three classes based on their privacy preferences: “privacy fundamentalists,” “privacy pragmatists,” and the “privacy unconcerned.”¹⁴ Westin's work frames the majority of consumers as “privacy pragmatists,” a form of privacy *homines economici*.¹⁵ He characterized this group as

considered to have created, almost single-handedly, the modern field of privacy law.”).

7. ALAN F. WESTIN, *PRIVACY AND FREEDOM* (1967).

8. *Id.* at 8–11 (“[M]en and animals share several basic mechanisms for claiming privacy among their own fellows.”).

9. *Id.* at 3.

10. *See id.* at 23 (“[C]ertain patterns of privacy, disclosure, and surveillance are functional necessities for particular kinds of political regime.”).

11. *See id.* at 3.

12. *Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Subcomm. on Commerce, Trade & Consumer Prot. of the H. Comm. on Energy & Commerce*, 107th Cong. 15 (2001) [hereinafter *Opinion Surveys*] (statement of Alan F. Westin, Professor Emeritus, Columbia Univ., President, Privacy and Am. Business), available at <http://www.gpo.gov/fdsys/pkg/CHRG-107hhr72825/pdf/CHRG-107hhr72825.pdf>.

13. *See infra* note 19.

14. *Opinion Surveys*, *supra* note 12, at 15–16.

15. *See id.* at 16 (stating that 63% of American adults are “privacy pragmatists”).

supporting a leave-it-to-the-market approach and as operating according to a rational choice model that expects consumers themselves to negotiate privacy in the marketplace.¹⁶

Westin's survey research work was largely descriptive and tailored to address public policy.¹⁷ Unlike his formal academic work, Westin rarely published his survey research in academic journals.¹⁸ Many of the surveys concerned the issues important to their various sponsors¹⁹ and are no longer available online.²⁰ Most are thus

16. See *id.* (stating that "privacy pragmatists" weigh and consider the benefits and risks of providing personal information, as well as the safeguards a company has in place and the level of trust they have in the company).

17. See ALAN F. WESTIN & MICHAEL A. BAKER, *DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY* 337-405 (1972) (discussing public policy implications of one of Westin's studies). But see *Opinion Surveys*, *supra* note 12, at 17 ("[S]urveys are not a very good way to write legislation.").

18. For the most prominent discussion by Westin of his survey research in the academic literature, see generally Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES 431 (2003).

19. A report for the American Institute of Certified Public Accountants ("AICPA") and Ernst & Young concluded, "Retaining an independent auditing firm to verify that a website is doing what it promises in the company's privacy policies tops the list of actions businesses could take to instill confidence in consumers." HARRIS INTERACTIVE, *PRIVACY ON AND OFF THE INTERNET: WHAT CONSUMERS WANT* 26 (2002), available at <http://www.ijsselsteijn.nl/slides/Harris.pdf>. A report for telecommunications company Ameritech concluded, "Sixty-nine percent of consumers say it is acceptable for local telephone companies to look at patterns of customer use of telephone services and draw on these to decide which customers would receive offers of new or additional telephone-related services." Alan F. Westin, *The Era of Consensual Marketing is Coming*, *PRIVACYEXCHANGE* (Dec. 14, 1998), <https://web.archive.org/web/19990827022529/http://www.privacyexchange.org/iss/surveys/1298essay.html>. A report for the online advertising firm DoubleClick concluded, "A majority of Internet users (61%) say they would be positive toward receiving banner ads tailored to their personal interests rather than receiving random ads." *DoubleClick Survey Executive Summary*, *PRIVACY & AM. BUS.*, <https://web.archive.org/web/20000819020002/http://www.pandab.org/doubleclicksummary.html> (last visited Apr. 5, 2014). A report for the consulting firm PricewaterhouseCoopers concluded, "Net users and computer users say that a privacy auditing procedure of company websites conducted by an independent accounting firm to ensure that privacy standards were adopted by business, along with a public report of the findings, would substantially increase their confidence in using such websites." *E-Commerce Privacy Survey Executive Summary*, *PRIVACYEXCHANGE* (Nov. 10, 1998), <https://web.archive.org/web/20060924011835/http://www.privacyexchange.org/iss/surveys/ecommsum.html>. A study conducted for Pacific Telesis concluded that consumers supported the marketing use of their telephone records. *Implementation of the Telecomms. Act of 1996: Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info.*, 13 FCC Rcd. 8061, 8107-08 (1998). See generally Oscar H. Gandy, Jr., *Public Opinion Surveys and the Formation of Privacy Policy*, 59 J. SOC. ISSUES 283, 289 (2003) ("It seems likely that the credibility of Alan Westin as a noted privacy scholar justified the prominent linkage of his name with a series of corporate sponsored

difficult to find.²¹ As a result, this survey work has rarely undergone serious academic review or critique, and the small amount that has occurred²² appears to have gone unanswered by Westin.

In Parts I and II of this Article, we describe the Westin segmentation, report on survey-based empirical tests of it, and engage in three critiques. Our data both present an updated picture of Americans' knowledge about, and attitudes toward, informational privacy, and challenge the Westin segmentation.

Our first critique, in Subpart II.A, is grounded in an examination of the sorting methodology Westin used to segment consumers, and a textual analysis of the questions used. It examines the logic, assumptions, and qualification language Westin used to describe different kinds of consumers, and his method of using the privacy pragmatist category as the default.

The second and third critiques are empirical. In Subparts II.B and II.C, we present original data from nationwide, telephonic surveys of Internet and mobile phone users collected over four years, in each case repeating the Westin segmentation questions and probing consumers' knowledge about and attitudes toward a series of technological attributes and marketplace offerings. The second critique is based on our finding of an apparent knowledge gap among consumers concerning business practices and legal protections for privacy, calling into question consumers' status as pragmatic. The third critique is based on presenting survey respondents with a series of privacy choices in the marketplace, focusing on location and other data sharing made possible by wireless phones. We find that privacy pragmatists act differently from Westin's model when directly presented with the value

privacy surveys."); Glenn Simpson, *Consumer-Privacy Issue Turns a Retired Professor into a Hot Item*, WALL ST. J., June 25, 2001, at A20 ("[Westin] is on the payrolls of many of the large financial services, technology and marketing companies that have resisted new privacy rules and legislation, including GlaxoSmithKline PLC, Equifax Inc. and First Data Corp. In addition to being consulting clients, Merck & Co., Visa International's Visa USA unit, DoubleClick Inc. and Verizon Communications are among the contributors to his nonprofit research group, the Center for Social and Legal Research.").

20. In 2005, Ponnurangam Kumaraguru and Professor Lorrie Faith Cranor attempted to summarize different versions of Westin's privacy segmentation and were only able to locate six of thirty extant surveys. PONNURANGAM KUMARAGURU & LORRIE FAITH CRANOR, *PRIVACY INDEXES: A SURVEY OF WESTIN'S STUDIES 3* (2005), available at <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf>.

21. *Id.*

22. See, e.g., Oscar H. Gandy, Jr., *The Role of Theory in the Policy Process: A Response to Professor Westin*, in *TOWARD AN INFORMATION BILL OF RIGHTS AND RESPONSIBILITIES* 1, 104 (Charles M. Firestone & Jorge Reina Schement eds., 1995).

exchange—and thus the privacy tradeoff—offered with these services.²³

In Part III, we come to two general conclusions. First, our combined findings and resulting analysis reframe the privacy pragmatist and call her influential status in U.S. research, industry practice, and policy into serious question. Under the new view, she cannot be seen as “pragmatic” at all, but rather as a consumer making choices in the marketplace with substantial deficits in her understanding of business practices.

Under this framework, policy prescriptions grounded in an expectation of bargaining by “privacy pragmatists” are misguided and counterproductive, because the knowledge gap that consumers experience undermines their abilities to choose services consistent with their preferences in the marketplace. Operating under this limited view of their choices and their duties as consumers, individuals may have both little ability to bargain for privacy in the marketplace and little reason to do so, as they believe legally enforceable rights protect them by default.

Second, we urge a more complete look at Westin’s body of work, and a reinvigoration of his broader legacy. *Privacy and Freedom* concludes with a broad discussion of public-policy choices for the country.²⁴ Westin neatly summarized his views in a 1995 policy report under a heading that signaled his view that bad privacy outcomes are not determined by technology:

Conclusion: The Choices Remain With Us, Not the Machines

... If we mean to do so, we can design information systems that give each person more choices as to the uses or nonuses of data than were ever feasible or cost-effective before

In short, the balances we will set in the United States for privacy rights, information-disclosure duties, and limited surveillance authority in the next era of the Information Age will remain—as they have always been—a part of democratic politics, anchored in the inevitable conflicts over social values, economic power, and organizational-individual relationships in a free society.²⁵

After publishing *Privacy and Freedom*, Westin consistently espoused a theory in which human-made privacy choices were

23. See generally Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, in DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363, 370–73 (Alessandro Acquisti et al. eds., 2008).

24. *Id.*

25. Alan F. Westin, *Privacy Rights and Responsibilities in the Next Era of the Information Age*, in TOWARD AN INFORMATION BILL OF RIGHTS AND RESPONSIBILITIES, *supra* note 22, at 94.

necessary to good technology and business practice decisions.²⁶ This broader theory has long been eclipsed by his survey work's support for the notice-and-choice model. Yet in the current environment of rapid-fire changes to technologies, services, and both industry and government collection and use of data, Westin's broader conclusions resonate strongly. Policymakers, industry, and academe would do well to resurrect them.

I. THE WESTIN PRIVACY SEGMENTATION

Westin's privacy segmentation divides the American public into three groups: the privacy fundamentalists (high privacy concern and high distrust in government, business, and technology), the privacy pragmatists (mid-level concern and distrust), and the privacy unconcerned (no or low concern and distrust).²⁷ For many years, academics from a variety of different disciplines have used the Westin segmentation for privacy analysis. For example, it has recently been employed in psychology,²⁸ in the study of marketing,²⁹ in computer security,³⁰ and in the information and communications technology contexts.³¹

In 2001 written testimony before Congress, Westin made the clearest extant summary of these three groups:

Privacy Fundamentalists [about 25%]: This group sees privacy as an especially high value, rejects the claims of many organizations to need or be entitled to get personal information for their business or governmental programs, thinks more individuals should simply refuse to give out information they are asked for, and favors enactment of strong federal and state laws to secure privacy rights and control organizational discretion. . . .

26. See, e.g., WESTIN & BAKER, *supra* note 17 (discussing privacy-related concerns with computerized record-keeping); Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?*, 72 CHI.-KENT L. REV. 271 (1996) (discussing employees' expectations and businesses' choices regarding privacy in the workplace).

27. *Opinion Surveys*, *supra* note 12, at 15–16.

28. 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. & TECH. 157, 157–58 (2007).

29. Sara Dolnicar & Yolanda Jordaan, *A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing*, 36 J. ADVERTISING, Summer 2007, at 123, 126.

30. ANDREW BESMER ET AL., SOCIAL APPLICATIONS: EXPLORING A MORE SECURE FRAMEWORK 5 (2009), available at <http://hci.uncc.edu/pubs/socialapplications.pdf>.

31. Mike Bergmann, *Testing Privacy Awareness, in THE FUTURE OF IDENTITY IN THE INFORMATION SOCIETY* 237, 247 (Vashek Matyáš et al. eds., 2009).

Privacy Unconcerned [about 20%]: This group doesn't know what the "privacy fuss" is all about, supports the benefits of most organizational programs over warnings about privacy abuse, has little problem with supplying their personal information to government authorities or businesses, and sees no need for creating another government bureaucracy . . . to protect someone's privacy. . . .

Privacy Pragmatists [about 55%]: This group weighs the value to them and society of various business or government programs calling for personal information, examines the relevance and social propriety of the information sought, wants to know the potential risks to privacy or security of their information, looks to see whether fair information practices are being widely enough observed, and then decides whether they will agree or disagree with specific information activities—with their trust in the particular industry or company involved a critical decisional factor. The pragmatists favor voluntary standards and consumer choice over legislation and government enforcement. But they will back legislation when they think not enough is being done—or meaningfully done—by voluntary means.³²

A. *The Privacy Pragmatist as Homo Economicus*

Westin consistently explained the American consumer using rational choice theory, with a focus on individuals maximizing their expected utility in the market through consumer choices.³³ For example, in the oral testimony cited above, one of Westin's four major policy observations was that "[t]he great majority of consumers favor a notice and choice approach to privacy policies."³⁴ Under headings such as "Most Consumers Are Shrewd Privacy Balancers," Westin argued that Americans examined product offerings to see whether businesses followed responsible information practices and made decisions accordingly.³⁵ According to this theory, these individual decisions create a collective crucible in which the success or failure of products and services is decided, culminating in macro-level effects on societal levels of information privacy.³⁶ Reflecting his research, Westin argued in his written testimony that the most influential decisions are made by the privacy pragmatists, whose preferences can steer a product to

32. KUMARAGURU & CRANOR, *supra* note 20, at 14.

33. For a basic introduction to the range of theories labeled "rational choice," see generally STEPHEN PARSONS, *RATIONAL CHOICE AND POLITICS: A CRITICAL INTRODUCTION* 6 (2005).

34. *Opinion Surveys*, *supra* note 12, at 18.

35. Alan F. Westin, *Intrusions: Privacy Tradeoffs in a Free Society*, *PUB. PERS.*, Nov.–Dec. 2000, at 8, 10.

36. *Opinion Surveys*, *supra* note 12, at 18–19.

success or ruin.³⁷ As such, Westin argued that the overall politics of privacy flows from privacy pragmatists' marketplace decisions.³⁸

It is surely right that consumers' choices in the marketplace influence the success or failure of products and services, including those that have an impact on privacy. Westin's theory is further attractive in its assumptions of how this happens. The theory recognizes the potential sophistication of individual consumers and vests trust in the competence of the average consumer. Westin argued that consumers applied "pretty sophisticated notions of relevance" in accepting practices such as credit reporting, and that for "most Americans, the key issue is almost always a matter of defining, adopting, and observing reasonable safeguards to avoid or limit present or potential abuses."³⁹

Overall, the Westin approach supports the idea that most individuals are privacy rationalists who knowledgeably weigh costs and benefits and make marketplace decisions that, overall, steer the consumer economy toward a compromise that balances societal concerns about privacy with the advance of technology. This general theory is reflected in, for example, the longstanding U.S. policy choice to forego comprehensive data protection schemes or similar regulatory approaches in favor of consumer-choice-based models of informational privacy.

We wondered whether this narrative was right. In the next Part, we consider this question via textual analysis and through our own survey instruments.

II. CRITIQUING WESTIN'S PRIVACY *HOMO ECONOMICUS*

We considered the strength of Westin's underlying assumptions and methods in exploring his work's positive influence on the consumer-as-rationalist narrative. We employ two methods in our analysis. First, we consider the text of the instrument Westin employed. Second, we consider results from testing the Westin segmentation using successive fieldings of the Berkeley Consumer

37. Westin argued that the political economy of privacy is shaped by the privacy pragmatists:

In the politics of privacy, the battle is for the hearts and minds of the Privacy Pragmatists. If most of them feel their personal information is being used fairly and properly by businesses, especially online, they join the Privacy Unconcerned to make up a 75% level support for the existing rules and practices. But if most of the Privacy Pragmatists feel that information practices are intrusive or their information is being misused, they join the Privacy Fundamentalists to make up a majority seeking legislative or regulatory measures, or consumer boycotts.

Westin, *supra* note 35.

38. *Opinion Survey*, *supra* note 12, at 19.

39. Westin, *supra* note 35, at 11.

Privacy Survey. For both, we employed a version of the segmentation test that was used by Westin for at least six years. This version was used for the 2001 report and Westin's testimony before Congress that we cited above.⁴⁰

We found that this narrative appears flawed. The problems are threefold. First, upon examination, Westin's assumptions in categorizing consumers do not cohere logically: the segmentation cannot establish that consumers adhere to pragmatism. Second, under empirical analysis based on knowledge tests, the average consumer appears to operate in the marketplace with a flawed, yet optimistic, perception of business practices and legal protections that could lead to undermine her ability to choose effectively. Third, when presented with the value exchange of information for services behind a variety of new offerings in the mobile phone space, privacy pragmatists do not act as Westin predicted.

A. *Assumptions Underlying the Privacy Segmentation*

Our first critique focuses on the methods Westin used to categorize consumers as fundamentalists, pragmatists, or the unconcerned. Ponnurangam Kumaraguru and Lorrie Cranor have engaged in the most careful review of Westin's privacy segmentation, finding that Westin used different criteria and different answers for developing his framework at different times.⁴¹ We agree that there is value in administering consistent questions over time; however, there is also a need to tailor survey research and perfect it over years of testing. Thus, our critique is based on a different issue: whether the segmentation, as applied, can accurately qualify a consumer as a "pragmatist" and whether that qualification remains valid under testing.

The text asks respondents:

For each of the following statements, how strongly do you agree or disagree?

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.⁴²

40. For the text of these questions, see KUMARAGURU & CRANOR, *supra* note 20, at 14–15.

41. *Id.* at 3–4, 16, 19–20.

42. *Id.*

Kumaraguru and Cranor reported that Westin segmented the three groups as follows:

Privacy Fundamentalists are respondents who agreed (strongly or somewhat) with the first statement . . . and disagreed (strongly or somewhat) with the second . . . and third statements

Privacy Unconcerned are those respondents who disagreed with the first statement . . . and agreed with the second . . . and third statements

Privacy Pragmatists are all other respondents.⁴³

We question this segmentation process, as described, in several respects. First, it appears that Westin coded privacy pragmatists as the default category—"all other respondents." This is problematic as a matter of logic because pragmatism, as generally understood, requires its adherents to engage in positive inquiry, to weigh costs and benefits of different decisions, and to reject idealism in favor of practical means and obtainable ends.⁴⁴ It is unclear, at best, that a belief about whether consumers have control over personal information or about how "most" businesses handle personal information corresponds to a pragmatic approach to personal information privacy. It may also be that consumers simultaneously believe that "most" businesses fail to handle personal information in a "proper and confidential" way and fail to act on that belief in the marketplace as expected. Beliefs about control over personal information and business behaviors may inform, or may be completely orthogonal to, an individual's behavioral approach. This reasoning applies equally to privacy "fundamentalists" and the "unconcerned," who could simultaneously hold beliefs about business practice and law and remain "fundamentalist" or "unconcerned" in their attitudes about these beliefs. And all three groups may be misinformed in their beliefs, calling the decisional conclusion into question.

More specifically, Westin's questions asked individuals about their attitudes towards consumer control, business use of data, and existing law. None of these questions have much to do with the specific behaviors—evaluating and weighing choices and making a cost-benefit-driven decision—that define pragmatism. It is thus not possible to answer Westin's screening questions and come to the conclusion that privacy pragmatists "weigh the potential pros and cons of sharing information, evaluate the protections that are in place and their trust in the company or organization. After this,

43. *Id.* at 15.

44. *Pragmatism*, STAN. ENCYCLOPEDIA OF PHIL., <http://plato.stanford.edu/entries/pragmatism/> (last modified Oct. 7, 2013).

they decide whether it makes sense for them to share their personal information.”⁴⁵

Categorizing those who disagreed with the first statement and agreed with the second and third statements as “privacy unconcerned” presents similar methodological problems. One could imagine a consumer agreeing with the first question concerning a lack of control, yet being nonchalant about that lack of control. The “unconcerned” consumer may understand information practices as outside of her control and consider this unproblematic—the assumption made in the model. But there are a variety of other plausible explanations for her answer. She may, for example, consider loss of control a problem but rationalize it by trusting what she believes to be existing law and business practices for protection. The segmentation questions used to categorize her, which ask about whether both business practices and laws are sufficient, certainly could lead to this conclusion. Indeed, as we discuss further below, our survey findings suggest that consumers do not always understand businesses’ responsibilities or practices and sometimes expect protections that do not presently exist in U.S. law.⁴⁶ Further, most consumers have little choice but to trust that the services they use are secure and responsible because they cannot effectively monitor information security practices or police them.⁴⁷ But consumers’ inability to monitor and police does not equate to a lack of concern about privacy.

Categorizing those who agreed that consumers “had lost all control” over the use of personal information and disagreed that business practices or laws were sufficient protection as “privacy fundamentalists” again poses similar problems. For example, one’s overall attitude and preferences may be strongly weighted toward the value of privacy (i.e., treating privacy as a fundamental and necessary element), yet one may think that business practices and laws provide sufficient protection. Or those categorized as fundamentalists may simply have higher levels of knowledge about the levels of protection in place; as discussed below, this is indeed what we found for some types of protection.

Finally, to effectively segment groups, the segmentation questions should have objective answers. Question One considers

45. HARRIS INTERACTIVE, *supra* note 19, at 31.

46. *See infra* Subpart II.C.1.

47. Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet’s Most Popular Price*, 61 UCLA L. REV. 606, 611 (2014) (“Investment in security is entirely in the hands of the business—which has little incentive to invest the substantial resources necessary to protect consumer information. Consumers, in turn, have little ability to determine what security is adequate or whether businesses are complying with security rules. Even more problematically, security-breach notification requirements do not apply to most internet businesses.”).

whether consumers have “any” control over personal information. In a world of credit reporting⁴⁸ and pervasive online targeting,⁴⁹ one may logically come to the conclusion that individuals have little practical choice about information collection and use. The business community, led by Microsoft, recently released a paper arguing that such notions of control are antiquated, and has advocated a shift in regulation of data from collection and control to regulations focusing on how data are used.⁵⁰ Similarly, Michael Birnhack, among other academics, has recently identified control as a core challenge in protecting privacy.⁵¹ Ongoing reports of data breaches at private companies in the wake of reporting laws,⁵² along with recent revelations of National Security Agency and other government agency surveillance activities, may further contribute to a justified feeling that institutions rather than individuals are in control of data.⁵³ At the same time, consumers objectively can exercise some control in some limited domains (for example, by requesting corrections to mistakes on credit reports). Is this “any” control?

Similarly, Question Two probes whether the respondent believes businesses handle information in a “proper and confidential” way. On the one hand, this is strictly subjective—what is “proper” may vary widely from respondent to respondent. On the other hand, a consumer trying to employ an objective frame to answer the question presumably would have to answer in the negative. In U.S. law, businesses generally do not owe a duty of confidentiality to customers; this is an obligation limited to certain

48. The legislative bargain of the Fair Credit Reporting Act allows consumer reporting agencies to collect data on any individual, and these individuals cannot opt out of credit reporting itself. See 15 U.S.C. § 1681 (2012).

49. It is practically impossible to use Internet services and avoid the collection and use of information for advertising and other purposes. See generally Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273 (2012) (discussing tracking technologies used by advertisers).

50. FRED H. CATE & VIKTOR MAYER-SCHÖNBERGER, NOTICE AND CONSENT IN A WORLD OF BIG DATA 4–6 (2012), available at <http://download.microsoft.com/download/9/8/F/98FE20D2-FAE7-43C7-B569-C363F45C8B24/Microsoft%20Global%20Privacy%20Summit%20Report.pdf>.

51. Michael Birnhack & Nin Ahituv, *Privacy Implications of Emerging & Future Technologies* (forthcoming 2013) (manuscript at 32), available at <http://ssrn.com/abstract=2364396>.

52. See generally *Chronology of Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, <https://www.privacyrights.org/data-breach> (last updated Dec. 31, 2013) (organizing and reporting on data breaches nationwide).

53. See generally *The NSA Files*, THEGUARDIAN, <http://www.theguardian.com/world/the-nsa-files> (last visited Apr. 5, 2014) (presenting a collection of articles on the NSA's actions including phone and Internet interception and corporate cooperation with intelligence agencies.)

professions.⁵⁴ Indeed, many businesses' ordinary practices, such as customer list rental and sharing, would violate confidentiality norms.⁵⁵ The fact that consumers may not be aware of this in practical or legal terms further increases the uncertainty left by the question.

Question Three probes respondents' comfort with existing regulations and business practices. While this question also fails to necessarily map the pragmatic or nonpragmatic behavioral choices, it does promise to capture attitudes about privacy protections as understood by respondents. But as we explain below, our empirical findings suggest that a knowledge gap exists between actual business practices, legal protections, and individuals' notions of those practices and protections. This raises questions about how comfortable individuals would be with existing laws and practices if they were fully informed of their scope and limitations. We conceptualize this knowledge gap as creating a kind of marketplace "myopia," which causes consumers to misunderstand their duties under the notice and choice approach and distorts the market for privacy.

*B. Empirical Critiques of the Privacy Segmentation:
Categorization Errors and Knowledge Gaps*

Since 2009, we, along with researchers Joseph Turow, Jennifer King, and statistician Su Li, have deployed a series of nationwide consumer surveys probing Americans' understandings and attitudes about information flows and privacy,⁵⁶ which we collect into the Berkeley Consumer Privacy Survey. Each time, we have deployed Professor Westin's privacy segmentation questions along with a variety of knowledge tests and attitudinal questions, allowing us to test the segmentation questions.

54. See generally Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 135, 157–58 (2007) (discussing the history of confidential relations and situations where courts have found there to be a duty of confidentiality).

55. We realize that it may be unlikely for consumers to know the details of when a duty of confidentiality exists, or indeed, the difference, legally, between "confidentiality" and other forms of protection—but unfortunately, that is also part of the reason why Question Two is not likely to be predictive.

56. Decades of consumer survey research shows that Americans care about privacy. For an overview of research in this field, see generally Samuel J. Best et al., *Privacy in the Information Age*, 70 PUB. OPINION Q. 375, 375 (2006) ("[T]he polls show that concern about threats to personal privacy has been growing in recent years."); James E. Katz & Annette R. Tassone, *Public Opinion Trends: Privacy and Information Technology*, 54 PUB. OPINION Q. 125 (1990) (noting a rise in public concern over privacy issues involving information technology).

Our research casts Westin's narrative in a new light. Throughout the Berkeley survey series, we have found that American consumers take actions to protect their privacy, reject a variety of business models that require offering personal information to receive a benefit, tend to express a desire for legal privacy rights that do not presently exist, and importantly, appear to operate in the marketplace with a "knowledge gap" concerning existing legal protections and actual business practices.

This knowledge gap was first observed empirically by Professor Joseph Turow, who, starting in 2003, surveyed Americans about their knowledge of common Internet business practices, finding that:

the overwhelming majority of U.S. adults who use the internet at home have no clue about data flows—the invisible, cutting edge techniques whereby online organizations extract, manipulate, append, profile and share information about them. Even if they have a sense that sites track them and collect individual bits of their data, they simply don't fathom how those bits can be used. In fact, when presented with a common way that sites currently handle consumers' information, they say they would not accept it. The findings suggest that years into attempts by governments and advocacy groups to educate people about internet privacy, the system is more broken than ever.⁵⁷

We picked up this thread in the Berkeley Consumer Privacy Survey project. Since 2009, the project has fielded five consumer surveys—one in 2009, one in 2012, and three in 2013.⁵⁸ In each of the surveys, we employed Westin's three screening questions to segment our respondents into pragmatists, fundamentalists, and the unconcerned, and then probed consumers' knowledge and preferences for a variety of specific issues that changed as the marketplace changed. Finally, for a number of the questions, we mapped these consumers onto Westin's privacy segmentation in order to test its validity.

57. JOSEPH TUROW, AMERICANS & ONLINE PRIVACY: THE SYSTEM IS BROKEN 3 (2003), available at http://editor.annenbergpublicpolicycenter.org/wp-content/uploads/20030701_online_privacy_report2.pdf; JOSEPH TUROW ET AL., OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE 3 (2005), available at http://editor.annenbergpublicpolicycenter.org/wp-content/uploads/Turow_APPC_Report_WEB_FINAL2.pdf. This research is compiled and summarized in Joseph Turow et al., *Consumers' Understanding of Privacy Rules in the Marketplace*, 42 J. CONSUMER AFF. 411 (2008).

58. Our analysis of the 2013 data is ongoing. It also used a slightly different sample size and qualification language (all Internet users) to recruit participants, but is sufficiently comparable for our purposes here.

We first discuss our results with the Westin segmentation questions over the course of all five surveys, and then turn to questions asked in individual surveys to deepen the analysis. Questions reported here can be found in the appendices, as well as in the tables and text of Subpart II.C.

C. Results

1. Establishing the Segmentation and Comparing it to Privacy Concern

As a threshold matter, we repeated the Westin segmentation, as well as general questions asking about respondents’ level of concern about privacy issues, in each survey. We found similar proportions of “pragmatists,” “fundamentalists,” and “unconcerned” each time we fielded the questions, as shown in Table 1:

TABLE 1: SEGMENTATION SCREENER QUESTIONS

(Please tell me if you strongly agree, disagree, or strongly disagree with these statements.)

	<i>Strongly agree</i>	<i>Agree</i>	<i>Disagree</i>	<i>Strongly disagree</i>	<i>DK/Ref</i>
Consumers have lost all control over how personal information is collected and used by companies.					
11/13	23	42	27	4	4
9/13	28	40	24	4	3
8/13	25	47	22	4	3
2/12	24	45	25	4	2
7/09	20	47	27	4	2
Most businesses handle the personal information they collect about consumers in a proper and confidential way.					
11/13	5	47	32	11	4
9/13	8	46	30	11	4
8/13	8	48	31	10	4
2/12	6	52	30	8	4
7/09	5	53	32	6	4
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.					
11/13	4	43	36	13	5
9/13	6	40	36	12	5
8/13	6	48	31	12	3
2/12	5	50	32	8	4
7/09	4	50	34	8	4

We also asked about levels of general concern regarding Internet privacy issues in each survey. As shown in Table 2, we found a relatively stable level of concern and similar reasons for

growing concern. Strikingly, around 60% of respondents said that they were "more concerned" about privacy issues on the Internet than they had been five years before. Further, this growing concern is connected to people learning more about privacy risks online. Between 40% and 49% of respondents whose concern had grown cited this as the most important reason for the shift in their concern.

TABLE 2: PRIVACY CONCERN COMPARED TO FIVE YEARS AGO

(Compared to five years ago, would you say you are more concerned about privacy issues on the Internet, less concerned, or that you have about the same level of concern?)

	<u>11/13</u>	<u>9/13</u>	<u>8/13</u>	<u>2/12</u>	<u>7/09</u>
More concerned	62	62	63	66	55
Less concerned	4	5	4	5	6
Same level	32	31	30	28	38
Don't know/Refused	2	2	3	1	1
	N=1003	N=1005	N=1002	N=1203	N=1000

(Please tell me which ONE of the following is the MOST important reason you are more concerned about privacy issues on the Internet than you were five years ago)

	<u>11/13</u>	<u>9/13</u>	<u>8/13</u>	<u>2/12</u>	<u>7/09</u>
You know more about privacy risks online (or)	40	47	42	47	49
You have more to lose if your privacy were violated (or)	26	27	23	33	29
You have had an experience that has changed your mind about privacy (or)	16	12	17	16	17
(DO NOT READ) Some other reason	14	13	12	2	3
Don't know/Refused	4	2	6	2	2
	(n=624)	(n=624)	(n=625)	(n=818)	(n=563)

While these findings are highly stable—within nine points throughout the fieldings—we note that concern "compared to five years ago" did noticeably increase between 2009 and 2012. In the 2012 survey, overall, 66% said that they were more concerned about privacy issues, 5% reported being less concerned, and 28% reported the same level of concern. Compared to our 2009 survey, the "more concerned" category gained 11%, while the same level and "less concerned" categories dropped by 10% and 1%, respectively. Westin's segmentation adds an interesting contour, as even the unconcerned say they are more concerned about privacy (52%) than

five years earlier. One plausible reason for this is the significant increase in news reporting about Internet privacy over those years, along with some notable data breach announcements in the wake of data-breach legislation; however, we cannot say from these data whether this is the case.⁵⁹

In all years, however, knowing more about privacy issues was the most frequently cited reason for being more concerned about privacy, ranging from 40% to 49%. In cross tabulating the 2012 results with the Westin segmentation, we found that 60% of the privacy unconcerned cited knowing more about privacy as the reason why they had grown more concerned. Overall, 33% said that they were more concerned because they had more to lose, and 16% reported that an experience caused them to be more concerned about privacy.

In 2012 and 2013, we also asked whether respondents were “more concerned about the collection and use of information by the government, by private companies, or by both the government and private companies?” In 2012, 66% chose both the government and private companies, while 19% chose private companies, and just 11% chose government only. When we followed up in our three 2013 surveys, we again found the same results:

TABLE 3: LOCATION OF PRIVACY CONCERN—GOVERNMENT VS. PRIVATE COMPANIES

	<i>11/13</i>	<i>9/13</i>	<i>8/13</i>	<i>2/12</i>
Government (or)	13	16	13	11
Private companies (or)	14	15	14	19
Both the government and private companies (or)	66	63	65	66
(VOL.) Neither	5	4	6	2
Don't know/Refused	2	2	2	2

Indeed, contrary to libertarian narratives about Americans being primarily concerned about privacy intrusions from the State, survey research has long suggested that Americans are concerned about both government and private-sector privacy violations. In a series of four surveys from 1985 through 1989, researchers found that a growing number of Americans were concerned about both government and private-sector privacy issues, with only 20% to 22% identifying only business as a privacy concern, and only 22% to 26% identifying government only as the concern.⁶⁰

59. We have more recently begun to ask respondents about the effect of news reporting but do not have data from 2009 and 2012 to compare.

60. Katz & Tassone, *supra* note 56, at 140.

2. *2009 Consumer Privacy Survey: Broad Support for Privacy Rights, Misunderstanding of Existing Legal Protections, and Consumer Optimism*

We first take up the 2009 survey, which author Hoofnagle fielded with Joseph Turow and Jennifer King. The survey is a commissioned nationwide survey⁶¹ of American Internet users. It found broad support for a series of possible privacy rights, including among younger users of the Internet.⁶² Several trends emerged from this 2009 work.

a. Preferences for Privacy

First, we found that a large majority of Americans reported engaging in some behavior to protect personal information.⁶³

61. Questions reported here can be found in Appendix A. The survey was conducted from June 18 to July 2, 2009, by Princeton Survey Research Associates International ("PSRAI"). PSRAI conducted telephone interviews with a nationally representative, English-speaking sample of 1,000 American adults living in the continental United States. A combination of landline ($n=725$) and wireless ($n=275$) random digit dial ("RDD") samples was used to represent all adults in the continental United States who have access to either a landline or cellular telephone. The interviews averaged twenty minutes. The overall response rates were a typical 18% for the landline sample and 22% for the cellular sample. Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is $\pm 3.6\%$ at the 95% confidence level. The survey was fully funded by the Rose Foundation for Communities and the Environment.

62. CHRIS HOOFNAGLE ET AL., HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES AND POLICIES? 3 (2010), available at <http://ssrn.com/abstract=1589864>. An archive of our consumer privacy work is maintained at *Berkeley Consumer Privacy Survey*, BERKELEY L., <http://www.law.berkeley.edu/privacysurvey.htm> (last visited Apr. 5, 2014).

63. Our survey was modeled on a June 2004 study by Westin, wherein he asked whether respondents engaged in a series of behaviors to protect privacy. Alan F. Westin, *Consumer Activism on Privacy: A Warning to U.S. Businesses and Guidance for Privacy Strategists*, PRIVACY & AM. BUS., July 2004, at 1, 1–6 (on file with authors). In the study, respondents were asked whether they had engaged in one of six actions to protect their privacy: (1) whether the respondent had refused to give information to a company because it was not really needed or was too personal (83%), (2) whether the respondent had asked a company to remove her name and address from any lists they use for marketing purposes (87%), (3) whether the respondent had asked a company not to sell or give her name and address to another company (81%), (4) whether the respondent had asked a company to see what personal information the company had about consumers (15%), (5) whether the respondent had decided not to register at a website because they found the privacy policy presented there to be too complicated or unclear (65%), and (6) whether the respondent had filed a complaint with a government agency about misuse of personal information (7%). *Id.*; see also Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 723, 742 (2007–2008).

Eighty-eight percent of Americans had refused to give information to a business or a company because they thought it was not really necessary or was too personal.⁶⁴ Thirty-nine percent reported erasing Internet browser cookies "often."⁶⁵ Fifty-six percent reported "changing [their] mind[s]" about making a purchase because of a privacy concern.⁶⁶ Twenty-eight percent reported that they checked their credit report at least every three months.⁶⁷

Second, a majority of respondents at the time reported that they were more concerned about privacy than in the past.⁶⁸ Fifty-five percent reported being more concerned about privacy issues on the Internet than five years earlier.⁶⁹ This question had no baseline; that is, it did not have an existing measure for privacy concern to which we could compare this observation. The finding, however, was still of interest because it gave us the opportunity both to start setting a baseline for privacy concern and to ask individuals why they were more concerned. Forty-eight percent based their concern on knowing more about privacy,⁷⁰ while 30% said they were more concerned because they had more to lose.⁷¹

Third, Americans wanted strong penalties for privacy transgressions. When given options for possible privacy fines, 69% chose the largest option offered, "more than \$2,500," when "a company purchases or uses someone's personal information illegally."⁷² When probed for nonfinancial penalties, 38% wanted companies to fund efforts to help consumers protect their privacy,⁷³ while 35% wanted executives to face prison terms for privacy violations.⁷⁴

Fourth, Americans wanted new privacy rights in their general, commercial transactions online. Sixty-eight percent responded in the affirmative when asked, "Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?"⁷⁵ Ninety-two percent thought there should be a law that "requires websites and advertising companies to delete all stored information about an individual."⁷⁶

64. HOOFNAGLE ET AL., *supra* note 62, at 10.

65. *Id.* at 13.

66. *Id.*

67. *Id.* at 14.

68. *Id.* at 15.

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.* at 16.

73. *Id.*

74. *Id.*

75. *Id.* at 11.

76. *Id.*

b. The Knowledge Gap

The 2009 survey also included a quiz⁷⁷ that explored respondents' knowledge about privacy rules surrounding popular online and offline transactions. The questions about online transactions probed respondents' assumptions about the rights that exist in privacy policies through a series of true or false questions. For instance, "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission."⁷⁸ The correct answer to this question is false; a privacy policy, in essence, is simply a statement of practices, which could (and often does) allow information-sharing with third parties.

In the marketplace, consumers can rarely verify basic attributes about products and services, so they often rely on other indicia of quality, such as brand, cleanliness of a business or restaurant, or certification programs. In general, these questions addressed a suspicion that consumers were not reading privacy policies and comparing service offerings across different companies. Instead, consumers might look to other signals of good practice, such as company reputation and whether a privacy policy existed, in order

77. *Id.* at 17. The answer to each question was false. The online questions were:

[1] If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.

[2] If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government.

[3] If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so.

[4] If a website violates its privacy policy, it means that you have the right to sue the website for violating it.

[5] If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission.

Id. The offline questions were:

[1] When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission.

[2] When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission.

[3] When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission.

[4] When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission.

Id.

78. *Id.*

to develop a sense of trust in a website, just as consumers use proxies in the offline world when selecting businesses or restaurants.

Overall, respondents failed the privacy knowledge quiz. Only 25% of respondents answered three or more of the five online questions correctly, and 38% answered three or four of the offline questions correctly. Indeed, 30% answered every one of the five online questions incorrectly, and 27% answered every one of the four offline questions incorrectly. Younger respondents did most poorly, with 42% answering none of the online questions correctly, and 50% answering none of the offline questions correctly.

In each of the online true or false questions, a privacy right was framed as being inherently available if a website had a privacy policy. The high level of failure to choose the correct "false" response signals that Internet users falsely believe that privacy policies convey specific, legally enforceable rights to users.

This work suggests a picture of an American public that—at least in 2009—preferred more privacy rights in the marketplace, while at the same time falsely believing that the mere presence of a privacy policy guarantees legally enforceable, strong rights to privacy. Overall, it suggests a public that believed stronger protections exist than do, and that preferred significantly stronger default privacy rights than reflected in current law.

3. 2012 Consumer Privacy Survey: Privacy Fundamentalists Perform Significantly Better on Privacy Quizzes

Building on the 2009 survey and an earlier survey of California residents discussed below, we commissioned another nationwide survey in 2012⁷⁹ to explore Americans' privacy knowledge, preferences, and attitudes, focusing on web tracking, mobile computing platforms, and mobile payments technologies. In this work, we continued to be interested in whether a "knowledge gap" about practices or protections might exist. As described above, we were concerned about the validity of the Westin segmentation as a descriptor of consumer behavior and choices and wished to probe the segmentation framework in more detail. Finally, we were interested

79. Our 2012 consumer privacy survey was based on telephone interviews with a nationally representative sample of 1,203 adult Internet users living in the continental United States. Telephone interviews were conducted by landline ($n=678$) and cell phone ($n=525$, including 235 without a landline phone). Princeton Survey Research Associates International conducted the survey in English from January 27 to February 12, 2012. Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is ± 3.4 percentage points. Questions reported here are provided in Appendix B. The survey was fully funded by the Nokia Corporation.

in improving the methods for understanding consumer privacy choices further to understand preferences regarding web and mobile services, data collection, and use.

We employed several methods for doing so. First, we again asked questions that test respondents' knowledge about privacy protections in the marketplace. Second, we combined these with questions that probe consumers' preferences and attitudes toward specific privacy choices or marketplace value propositions. This method allowed us to move from more abstract questions about preferences and attitudes to further understanding of consumer knowledge, and on to probing actual value propositions available in the marketplace.

To test the Westin segmentation, we ran the segmentation questions as written above and then cross tested them with knowledge questions. This allowed us to both check for a knowledge gap and, if such a gap existed, to see whether it had a relationship to the Westin segmentation categories.

According to the Westin segmentation, 19% of our respondents responded as privacy fundamentalists, 56% as privacy pragmatists, and 16% as privacy unconcerned. Eight percent could not be categorized under the segmentation because they failed to answer at least one of the three screening questions.⁸⁰ We also asked the respondents three true or false questions relevant to current debates about online privacy, replicated in Table 4. In all three cases, the majority answered incorrectly or "don't know," but a large minority selected the correct answer.

We then cross tested the results and found that when Westin's segmentation is applied and cross-referenced with knowledge, the "privacy fundamentalists" were significantly more likely to answer correctly than either of the other two groups. Both privacy pragmatists and the unconcerned answered incorrectly more frequently than the fundamentalists.

80. Determining how to address this population presents a conundrum. Following Westin's methods as described by Kumaraguru and Cranor, one would presumably place the uncategorized into the pragmatist bucket, as Westin defined pragmatists as all respondents who were *not* fundamentalists or the unconcerned. As described in *supra* text accompanying notes 43–45, that approach seems improper to us and so we analyze this population as a separate group.

TABLE 4: TRUE OR FALSE PRIVACY QUIZ, WITH CORRECT ANSWERS IN BOLD FONT (2012)

	<i>True</i>	<i>False</i>	<i>DK</i>	<i>Ref.</i>
1. When you use the Internet to learn about medical conditions, advertisers are not allowed to track you in order to target advertisements.	22	36	41	1
2. Free websites that are supported by advertising are allowed to sell information gathered from users of the site, even if they have a privacy policy.	40	19	40	*
3. When visiting free websites supported by advertising, you have the right to require the website to delete the information it has about you.	25	32	42	*

Privacy fundamentalists answered all three knowledge questions correctly in greater proportion than the other groups; all differences were significant at a p of .01 or better. Forty-nine percent of privacy fundamentalists answered question one correctly, versus 34% of pragmatists, 32% of the unconcerned, and 28% of the uncategorized group.⁸¹ Fifty-two percent of privacy fundamentalists answered question two correctly, versus 38% of pragmatists, 35% of the unconcerned, and 42% of the uncategorized group.⁸² Forty percent of privacy fundamentalists answered question three correctly, versus 30% of pragmatists, 35% of the unconcerned, and 22% of the uncategorized group.⁸³

This finding followed a smaller study by author Hoofnagle and Jennifer King, who observed a similar knowledge gap between privacy fundamentalists and other segments in an earlier, smaller study focused on Californians.⁸⁴ In that study, Hoofnagle and King found that in eight of nine questions probing privacy knowledge, privacy fundamentalists answered correctly more often than pragmatists or the unconcerned.⁸⁵

81. $\chi^2(9, N=1203) = 28.2137$; $p = 0.0101$.

82. $\chi^2(9, N=1203) = 38.1481$; $p = 0.0002$.

83. $\chi^2(9, N=1203) = 32.2188$; $p = 0.0016$.

84. CHRIS JAY HOOFNAGLE & JENNIFER KING, RESEARCH REPORT: WHAT CALIFORNIANS UNDERSTAND ABOUT PRIVACY OFFLINE 23 (2008), available at <http://ssrn.com/abstract=1133075>.

85. *Id.* (these were significant at the $p < .05$ level).

4. Consumer Choices in Light of Actual Business and Government Practices

Finally, we wanted to use our survey instruments to test consumer preferences for actual business propositions and specific legal protections, and employed the 2012 nationwide telephonic instrument to do this. In this survey, we focused on the privacy of mobile phones and mobile payment systems, as consumers are increasingly using mobile devices to access Internet resources.

The rich, location-aware information that can be collected by mobile phone platforms and “apps” could be used for a variety of attractive services, marketing, and business analytical purposes. As such, cell phone users are confronted with “privacy pragmatic” options every day, particularly if they use smartphones. Further, we expected that a great deal of data collection that occurs via mobile platforms—everything from precise and rich (even near-real-time) location data to information about buying preferences—is not necessarily visible to consumers who are being asked to make pragmatic decisions in the marketplace. At the same time, many new business propositions—for example, collecting a person’s location in order to offer her a targeted ad and a coupon discount—are surely attractive features of mobile platforms for both businesses and consumers. Accordingly, these features are interesting in themselves, and also potentially provide a useful lens for looking at Americans’ stated preferences.

a. Methods

In developing our questions, we used a specific method, suggested to us both by our critiques of Westin’s and others’ previous work, and some useful critiques by others of existing survey research (including some critiques of our own earlier work). The critique holds that, in general, survey research on privacy does not ask about specific business propositions as offered to consumers in the marketplace. Instead, questions usually ask about more general attitudinal preferences, a method that is critiqued as being too abstract.

We think this is a useful observation. Accordingly, our methods employ a combination of questions that test respondents’ knowledge about privacy protections in the marketplace and questions that probe consumers’ preferences and attitudes toward specific privacy choices or marketplace value propositions. This allows us to move from more abstract questions about preferences and attitudes to the questions in light of an actual value proposition available in the marketplace.

The critique, however, extends even to questions like ours because it is not the actual proposition as experienced in the marketplace. In response to this, we have two observations. First, marketplace transactions themselves are often abstract. The

attributes of the proposition might not be apparent to the consumer because firms may have strong incentives to limit information to the consumer and present the value proposition in the most attractive fashion. Rather, the data may be passively collected without input from the consumer, leaving companies with little information about reactions to the value proposition until the collection is discovered and consumers react either positively or negatively. Well-formulated survey questions can surface the proposition for consumers to consider neutrally. Second, research shows that consumers are vulnerable to a wide variety of cognitive and behavioral biases in the marketplace. Among other biases, they are more likely to make a choice that seems to provide some benefit in the moment, that seems necessary at the time, or that is presented to them as a requirement, whether or not it is in fact required.⁸⁶ This again limits the genuine knowledge a consumer might have about a value proposition as experienced in the marketplace.

We sought to address some of these challenges by using questions that describe data collection (for example, a contact list) and the reason for it (for example, in order to offer more social connections), and are framed as neutrally as possible. We therefore asked Americans about their preferences for engaging in information sharing for several specific marketing or service-oriented purposes that companies had already proposed or implemented, or that were likely in the near future. We note that this method is still constrained by a limit inherent to survey research—notably, the consumer is not actually being offered the actual benefit in the moment; as such, it is more theoretical than an offer in front of her in the marketplace. This limit is also a strength, however, as she is explicitly being given a choice that is often implicit, or invisible, in the marketplace. We were thus able to both offer the benefit and make the “ask” for information that the privacy pragmatist is asked to make under the *homo economicus* model.⁸⁷

We were especially interested in this in light of longstanding assumptions by Westin and others that consumer *homines economici* understand and choose among value propositions. In some cases, however, companies may prefer not to ask in advance—specifically because customers are likely to reject the value proposition if it is clearly explained. One salient example of this problem is elucidated by Douglas Edwards in his 2011 book about working at Google.⁸⁸ Edwards discusses Google’s first-party cookie policy:

86. There is a burgeoning field of behavioral economic and psychological research on consumer privacy decision making that points to a variety of these cognitive deficits. See generally Acquisti & Grossklags, *supra* note 23.

87. Our specific questions are in the appendices. See *infra* Appendix A–C.

88. DOUGLAS EDWARDS, I’M FEELING LUCKY: THE CONFESSIONS OF GOOGLE EMPLOYEE NUMBER 59 (2011).

What if we let users opt out of accepting our cookies altogether? I liked that idea, but Marissa [Mayer] raised an interesting point. We would clearly want to set the default as “accept Google’s cookies.” If we fully explained what that meant to most users, however, they would probably prefer *not* to accept our cookie. So our default setting would go against users’ wishes. Some people might call that evil, and evil made Marissa uncomfortable. She was disturbed that our current cookie-setting practices made the argument a reasonable one. She agreed that at the very least we should have a page telling users how they could delete their cookies, whether set by Google or by some other website.⁸⁹

This anecdote shows one reason why the market can fail to produce privacy-friendly options for consumers expected to act as *homines economici*. Even when companies know that consumers want more privacy, firms can have incentives to code less privacy-protective options by default. Firms may also have incentives to hide the privacy tussle. (Google could have implemented compromise approaches that preserved some privacy, by using session cookies or by choosing cookies that expired after some short amount of time, but it did not.)

The anecdote also speaks to those who criticize all survey research on privacy as incomplete—even if the value proposition is offered, as we chose to do in our survey—because it does not present the tradeoffs consumers experience in transactions. These critics argue that without a value judgment in terms of provision of services, consumers will always say that they value privacy and then act contrary to their aspirations in the marketplace.⁹⁰ As with any method, survey research does have important limitations. At the same time, while there certainly may be a mismatch between consumers’ expressed preference and their ultimate behavior, this critique misses the point that consumers may have no realistic privacy-friendly option and that popular services are almost always offered on a take-it-or-leave-it basis, with little information about the actual collection practices. In the Facebook example above, for instance, people were surprised by the contact list collection despite the fact that the feature was covered by Facebook’s privacy policy.⁹¹

Better information about the underlying value propositions offered by app makers and other service providers, and consumers’

89. *Id.* at 341.

90. See Tanzina Vega, *Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, N.Y. TIMES, Feb. 27, 2012, at B1.

91. Indeed, Facebook had previously updated its notice to make the Contact Sync feature explicit. See, e.g., Charles Arthur, *Is Your Private Phone Number on Facebook? Probably. And So Are Your Friends*, THEGUARDIAN (Oct. 6, 2010), <http://www.theguardian.com/technology/blog/2010/oct/06/facebook-privacy-phone-numbers-upload>.

attitudes towards them, would be beneficial to both consumers and companies. Service providers often downplay information collection, presenting the benefit of the service as a pure windfall to the consumer from viewing advertising. Thus, we chose to bring the information exchange implicit in these transactions into view. To do so, we created survey questions that describe specific forms of information collection as neutrally as possible, along with some questions that offer the respondent an actual value exchange that existed in the marketplace.

b. Data Collection via Mobile Phone Apps

Mobile phone apps can collect user information both directly and indirectly. Examples of direct collection include tracking posts to social networking sites, harvesting data input by users or their reading, viewing, and listening practices, and collecting information stored in other phone applications.⁹² Indirect collection includes harvesting information from other mobile users of the app who are connected to the smartphone's owner.⁹³

At least some app providers have configured their apps to collect data stored in other locations on the phone. In 2011, for example, Facebook garnered press attention for using its mobile app to collect contact lists from the phones of consumers who had the app installed.⁹⁴ Facebook used the contact lists to suggest additional "friend" contacts to those consumers.⁹⁵ When the practice came to light, however, consumers expressed outrage,⁹⁶ and today Facebook offers a click-through screen for consent.

The controversy over Facebook's contact list collection was followed in 2012—just after our survey was completed—by news that Path, another social networking company, was also uploading mobile address books to its servers via mobile phone apps without notice or consent, along with news that the practice was not limited

92. See, e.g., JENNIFER M. URBAN ET AL., *MOBILE PHONES AND PRIVACY* 15 (2012), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405 (collecting examples).

93. This information can be quite detailed, involving, for example, "social graph" profiling information. See, e.g., Graham Cluley, *How to Stop Your Friends' Facebook Apps from Accessing *Your* Private Information*, *NAKED SECURITY* (Apr. 3, 2013), <http://nakedsecurity.sophos.com/2013/04/03/how-to-stop-your-friends-facebook-apps-from-accessing-your-private-information> (describing the information shared by default based on friends' activities).

94. See, e.g., Dan Tynan, *Facebook's Phonebook Fiasco*, *ITWORLD* (Aug. 11, 2011, 7:00 AM), <http://www.itworld.com/it-managementstrategy/192399/facebooks-phonebook-fiasco> (describing the Facebook syncing feature).

95. *Id.*

96. See Nicole Perlroth & Nick Bilton, *Mobile Apps Take Data Without Permission*, *BITS* (Feb. 15, 2012), http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/?_php=true&_type=blogs&_r=0.

to Facebook and Path.⁹⁷ In fact, close on the heels of the Path story were revelations that many app makers collected contact lists and stored them on their servers.⁹⁸

Backlash was swift, and included, among other reactions, a lawsuit against eighteen companies that allegedly collected contact data via apps,⁹⁹ a congressional demand that Apple appear and explain its role in the practice,¹⁰⁰ and a decision by Apple to update the iPhone iOS to allow access to contact data only with explicit consumer permission.¹⁰¹

Thus, companies may be well served by knowing consumers' baseline attitudes before commencing with features that may have an impact on privacy in order to offer the best choices in the marketplace. This holds true under a model in which consumers' roles as *homines economici* is assumed, but it should hold especially true if we assume that consumers are not adequately informed about privacy practices; in the past, information that was badly mismatched with consumer preferences has caused marketplace pain for companies offering new services, and in some cases, prevented the introduction of a new feature altogether, even if it could have been beneficial to consumers in a less privacy-damaging form.¹⁰²

Proceeding from this background, we asked Americans about two scenarios related to the mobile app privacy issues discussed above:

97. *Id.*

98. *Id.*

99. Chloe Albanesius, *18 Firms Sued over App Privacy, Including Apple, Twitter, Facebook*, PCMAG.COM (Mar. 15, 2012, 1:02 PM), <http://www.pcmag.com/article2/0,2817,2401625,00.asp>.

100. *See, e.g.*, Fahmida Y. Rashid, *Congress Demands Apple Clarify Mobile Privacy Policy*, PCMAG.COM (Mar. 15, 2012, 8:54 AM), <http://securitywatch.pcmag.com/mobile-apps/295412-congress-demands-apple-clarify-mobile-privacy-policy>.

101. *See, e.g.*, Sandhya Raman, *Amid Privacy Uproar, Apple Promises to Detail App Permissions*, FIERCEMOBILEIT (Feb. 15, 2012), <http://www.fiercemobileit.com/story/amid-privacy-uproar-apple-promises-detail-app-permissions/2012-02-15>.

102. The reactions to Facebook and Path's contact list collection, for example, brings to mind other examples—such as DoubleClick's year 2000 attempt to combine web tracking and offline information, and the Google Buzz rollout—in which failing to develop sufficient privacy practices and transparency at the outset created enough backlash to cause companies to substantially change their plans. Jay Greene, *Google's Buzz Kill Completes Shift to Google+*, CNET (Oct. 14, 2011, 10:47 AM), http://news.cnet.com/8301-1023_3-20120617-93/googles-buzz-kill-completes-shift-to-google/; Stefanie Olsen, *FTC Drops Probe into DoubleClick Privacy Practices*, CNET (Jan. 22, 2001, 5:35 PM), <http://news.cnet.com/2100-1023-251325.html>. Indeed, DoubleClick's shares lost nearly 90% of their value after the Federal Trade Commission opened an investigation. *Id.*

First, we asked whether respondents would be willing to share contact list information on their phones with a social networking app so that the app provider could suggest more connections. This scenario tracked Facebook's use of phone contact lists.

Second, we asked whether respondents would be willing to share contact list information with a coupon app they had already chosen to download so that it could also offer coupons to people included in the contacts list. This second scenario was based on existing coupon apps that collect contact lists and let users share coupons with contacts.¹⁰³

We chose these scenarios for three main methodological reasons. First, they both reflected actual business practices related to contact information stored on mobile phones engaged in or planned by app providers. Second, they each provided a clear value proposition for the consumer to consider: (1) provide contacts in order to receive more connection opportunities; (2) provide contacts in order for those contacts to also receive coupon benefits. Third, they did not suggest any further uses of the contact information outside the stated value proposition.

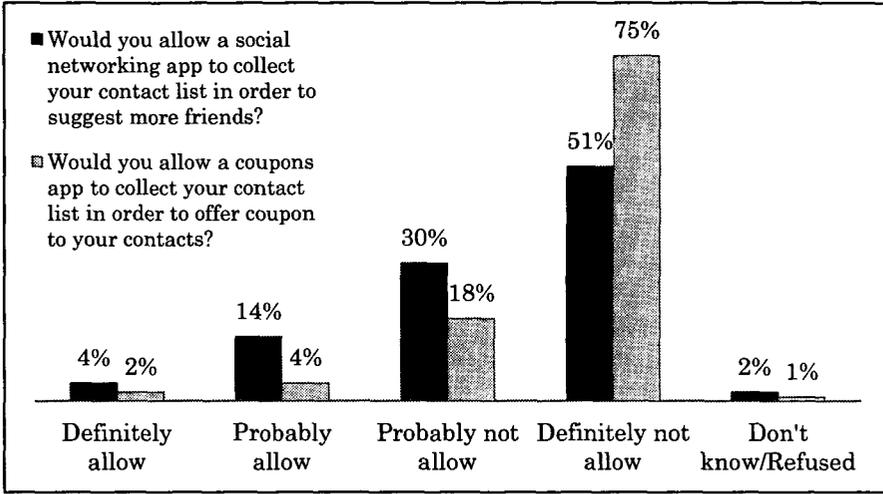
In taking this approach, we probably understated business data uses in these business models. While businesses sometimes use contact lists for other reasons that might trigger less adoption if known—for example, in constructing social graphs or other profiling information for advertising and marketing purposes—these additional reasons are not *necessarily* part of the value proposition. We wanted to understand respondents' attitudes toward the basic benefit offered, without suggesting more.

Respondents overwhelmingly rejected both scenarios. Eighty-one percent of respondents said they would "definitely not allow" (51%) or "probably not allow" (30%) sharing contact lists in order to receive more connection suggestions. Fourteen percent stated that they would "probably allow" this use of their contact lists, and only 4% stated that they would "definitely allow" it.

Rejection of the coupons app collection of contact list information was even stronger. Fully 93% of respondents said they would "definitely not allow" or "probably not allow" the coupons app to collect contact list information in order to suggest coupons to contacts; of these respondents, 75% "definitely would not allow" it. Only 4% would "probably allow" the collection, and only 2% would "definitely allow" it.

103. For a recent example, see *PhotoPon Makes Coupons Social: With App, Users Create Own Coupons for Friends and Family*, PRWEB (Mar. 29, 2012), <http://www.prweb.com/releases/PhotoPon/Coupon-App/prweb9347169.htm>.

FIGURE 1: WOULD YOU ALLOW APPS TO COLLECT YOUR CONTACTS?
(BASED ON CELL PHONE OWNERS, n=1119)



Given these results, it is perhaps unsurprising that the backlash against Path’s collection model was so strong.

c. Location Tracking via Mobile Phones: Data Collection, Consumer Retail Tracking and Profiling, Marketing Calls, and Targeted Coupons

Location awareness is one of the most attractive features of mobile phones for marketers, app providers, law enforcement, and consumers. Among many other possible uses, location awareness can allow law enforcement to track suspected criminals or missing persons, app makers to provide tailored mapping and direction information to consumers, and marketers to make location-specific offers to consumers.

As briefly described above, the location of mobile phone users can be tracked using a variety of methods, including methods that do not require the mobile phone user’s knowledge.¹⁰⁴ Additionally, highly accurate location data is routinely stored by telecommunications service providers.¹⁰⁵ The recent proliferation of technologies and services that take advantage of these location-tracking abilities presents an opportunity to research consumers’ attitudes and preferences towards a growing sector of information-intensive practices.

We also asked Americans some more general questions about location tracking and storing location information collected from

104. See *supra* text accompanying note 94–98.
105. URBAN ET AL., *supra* note 92, at 19.

mobile phones, as well as about the use of some of that information by retailers. Because we expect that consumer knowledge and attitudes about these practices might change over time, we repeated these questions in 2013.

First, we asked how long wireless service providers should retain the location data they collect about wireless phones on their network. We offered the following choices: less than a year; one to two years; two to five years; indefinitely; or not at all.¹⁰⁶

A plurality of respondents—46%—answered that wireless phone location data should not be kept at all. The next largest group—28% of respondents—answered that the data should be kept less than a year. Significantly fewer respondents chose longer retention timeframes, with 9% choosing one to two years, 6% choosing two to five years, and 7% choosing indefinite retention.

We repeated this question in 2013 and found similar numbers, though this time, respondents were more split between preferring that cell phone providers not keep the data at all and keeping it less than a year. Overall, 33% thought the data should not be kept at all, and 29% thought it should be kept less than a year. Seven percent chose two to five years, and 10% chose indefinite retention.

TABLE 5: HOW LONG SHOULD CELL PHONE PROVIDERS KEEP SUBSCRIBER LOCATION INFORMATION?

	<u>8/13</u>	<u>2/12</u>
Less than a year	29	28
One to two years	17	9
Two to five years	7	6
Indefinitely	10	7
Or should they not be able to keep it?	33	46
(DO NOT READ) Don't know/Refused	3	4
	(n=923)	(n=1119)

At the same time, retailers are rapidly adopting much broader and more complete phone-based tracking than data kept at the cell tower. During the 2011 Thanksgiving “Black Friday” sales weekend, some shopping centers and stores proposed or began to capture signals from consumers’ wireless phones to track them as they shopped and walked through retail locations.¹⁰⁷

106. These time periods were suggested to us by our survey research company. In general, respondents tend to consider anything longer than five years “indefinite.”

107. Sean Gallagher, *We're Watching: Malls Track Shopper's Cell Phone Signals to Gather Marketing Data*, ARS TECHNICA (Nov. 25, 2011, 4:15 PM),

These proposals almost immediately became controversial, and two shopping centers that enrolled in a tracking plan for the 2011 Black Friday weekend cancelled them.¹⁰⁸ In addition to generating this type of backlash due to business practices mismatched to consumer preferences, collecting such information from wireless phones may violate the federal Pen Register Act.¹⁰⁹

The possibility of tracking consumers in a store to understand their behavior, gauge their preferences, and offer them tailored ads represents a tempting proposition for retailers that could also be useful to consumers. The recent trend to begin tracking phone location for these purposes provides a useful example of an apparent mismatch between the strength and direction of consumers' actual preferences, compared to retailers' understandings of those preferences, that is amenable to probing in survey work. In 2013, another retailer, this time Nordstrom, quickly ended a practice of tracking shopper's phones using Wi-Fi after a posted notice generated consumer complaints.¹¹⁰ Nordstrom both gave notice (in the form of posted signs)¹¹¹ and was not using identified information for its tracking but was still the subject of backlash.¹¹²

While Nordstrom both gave notice and did not identify customers, other companies are exploring ways to track individuals uniquely through signals emitted from phones; these systems will not necessarily provide the customer with notice or a choice. One system developed by Euclid tracks consumers through the "MAC" ("Media Access Control") address that uniquely identifies a smartphone.¹¹³ The MAC address is transmitted whenever the consumer has Wi-Fi enabled.¹¹⁴ Similarly, Navizon I.T.S. claims that it can track "any Wi-Fi enabled smart phone or tablet, including iPhones, iPads, Android devices, BlackBerry, Windows

<http://arstechnica.com/business/2011/11/were-watching-malls-track-shoppers-cell-phone-signals-to-gather-marketing-data/>.

108. Annalyn Censky, *Malls Stop Tracking Shoppers' Cell Phones*, CNNMONEY (Nov. 28, 2011, 1:58 PM), http://money.cnn.com/2011/11/28/news/economy/malls_track_shoppers_cell_phones/index.htm.

109. 18 U.S.C. § 3121 (2012).

110. Aaron Pressman, *Privacy Advocates Worry over New Apple iPhone Tracking Feature*, YAHOO! (Jan. 10, 2014, 4:07 PM), <http://finance.yahoo.com/blogs/the-exchange/privacy-advocates-worry-over-new-apple-iphone-tracking-feature-161836223.html>.

111. Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES, July 15, 2013, at A1.

112. Pressman, *supra* note 110.

113. *Privacy Statement*, EUCLID (Jan. 9, 2014), <http://euclidanalytics.com/privacy/statement/>.

114. *Id.*

Mobile and Symbian, as well as laptops and all Wi-Fi tags.”¹¹⁵ As with many other tracking technologies, Navizon’s seems to be designed to operate without the knowledge of the individual being tracked.¹¹⁶ Under its “unobtrusive surveillance” feature section, Navizon claims that “Navizon I.T.S. works in the background, quietly and unobtrusively locating Wi-Fi-enabled devices. . . . No application is needed on the devices to be tracked. The only requirement is that their Wi-Fi radios be turned on, which is the default in most smart phones, tablets and laptops.”¹¹⁷

If information about the phone is combined with other data, it is very likely that individuals will be identified based on their phone’s attributes. Individuals can be monitored and identified through unique IMSI (“International Mobile Subscriber Identity”) numbers, which, like MAC addresses, are embedded in users’ phones and are transmitted during normal use of the device.¹¹⁸ In order for consumers to prevent tracking based on these technologies, they must either disable the Wi-Fi on their phones (in the case of MAC address tracking) or turn off their phones entirely (if IMSI catchers are being employed).

Indeed, in recent months, news of new tracking offerings—along with consumer complaints—has only increased as stores move to work with services like Retail-Next and Nomi, which provide technology to help stores analyze consumer traffic patterns, create behavioral profiles, and customize offers based on uniquely identifying customers’ phones.¹¹⁹ Retail-Next claims to be able to collect approximately 10,000 data points per store visitor¹²⁰—an enormous amount of information that could easily be re-identified to the phone owner, even if a store does not at first make the connection. *LifeHacker* reports, for example, on the kind of information commonly collected:

Since the surveillance system varies from store to store, the amount of information each retailer collects can vary. However, most stores use your phone’s MAC address to identify you, and records when you enter and leave a store,

115. *Navizon Indoor Triangulation System*, NAVIZON, <http://www.navizon.com/product-navizon-indoor-triangulation-system> (last visited Mar. 10, 2014).

116. *See id.*

117. *Id.*

118. Thomas A. O’Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. ATTY’S BULL., Nov. 2011, at 16, 20, http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

119. Lisa Wirthman, *What Your Cellphone Is Telling Retailers About You*, FORBES (Dec. 16, 2013, 11:27 AM), <http://www.forbes.com/sites/emc/2013/12/16/what-your-cellphone-is-telling-retailers-about-you/>.

120. *Id.*

where you go inside the store, and how long you pause to inspect specific products, aisles, and counters. Combined with video surveillance, those stores also collect your gender and demographics (ethnicity/general age/anything that can be determined visually), differentiate children from adults, note specific products you looked at and how long you looked at them, and so on.¹²¹

All in all, location-based tracking and profiling using mobile phones provides a rich opportunity for testing new, privacy-relevant business propositions that consumers are asked to consider in the marketplace. This gives us a useful foundation upon which to consider Westin's market segmentation model using real-world business propositions.

As such, in the 2012 survey, we asked Americans several questions about this location-based tracking of their movements and habits while in stores. First, we asked whether they thought that phones should share information with stores when they visit and browse without making a purchase. Overwhelmingly, subjects rejected this possibility. Ninety-six percent objected to such tracking, with 79% stating that they would "definitely not allow" it and 17% stating that they would "probably not allow" it.

Because, as noted above, the clamor to use these technologies has only grown since 2012, we again queried consumers about it in August 2013. To improve its match to the technology as it is developing and to correct for any bias introduced by the phrase "only browsing," we tailored the question to more directly describe the sharing and to instead refer more generally to being "out shopping."

TABLE 6: WOULD YOU ALLOW YOUR CELL PHONE PROVIDER OR APPS ON YOUR PHONE TO SHARE INFORMATION ABOUT YOU WITH THE STORES THAT YOU VISIT WHILE YOU ARE OUT SHOPPING?

	<i>8/13</i>
Definitely allow	2
Probably allow	9
Probably not allow	18
Definitely not allow	70
Don't know/Refused	1
	(n=923)

Consumers continued to reject this type of tracking in high numbers. Eighty-eight percent objected, with 70% stating that they

121. Alan Henry, *How Retail Stores Track You Using Your Smartphone (and How to Stop It)*, LIFEHACKER (July 19, 2013, 4:00 AM), <http://lifehacker.com/how-retail-stores-track-you-using-your-smartphone-and-827512308>.

would “definitely not allow” it and 18% stating that they would “probably not allow” it. It is possible that the rise in the small minority of respondents who “probably” or “definitely” allow the sharing—from 4% to 11%—is because of the question’s reformulation or because of greater familiarity with the idea, but we cannot tell.

Second, we asked respondents whether they would allow wireless service providers to use their locations to tailor advertising to them. Despite the possible usefulness of ads that respond to a consumer’s location, this was also overwhelmingly rejected. Overall, 92% of respondents said that they would “definitely” or “probably” not allow the use of location data for this purpose. (Seventy percent stated they “definitely” would not allow it, and 22% stated they would “probably” not allow it.) Only 7% would “probably allow” the use of location to tailor ads, and only 1% would “definitely” allow it.

Because the technology behind location-aware ads—and the marketplace implementation of it via web tracking and mobile apps—has grown rapidly since we fielded the 2012 survey, we also repeated this question in August 2013, to very similar results. In this case, 83% of respondents said that they would “definitely” or “probably” not allow the use of location data to serve location-aware ads. (Sixty-six percent stated they “definitely” would not allow it, and 17% stated they would “probably” not allow it.) Though we cannot tell from such a small change, there has, perhaps, been a slight growth in the small minority who would allow this use of location data: 11% would “probably allow” the use of location to tailor ads, and 4% would “definitely” allow it. Overwhelmingly, however, respondents still rejected the use.¹²²

TABLE 7: WOULD YOU ALLOW YOUR CELL PHONE PROVIDER TO USE YOUR LOCATION TO TAILOR ADS TO YOU?

	<u>8/13</u>	<u>2/12</u>
Definitely allow	4	1
Probably allow	11	7
Probably not allow	17	22
Definitely not allow	66	70
Don't know/Refused	2	1
	(n=923)	(n=1119)

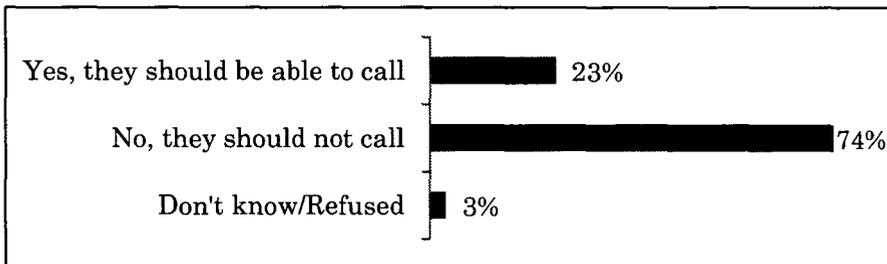
122. As mentioned above, the 2013 survey had a different sample size and a different method with which to qualify participants. We are thus hesitant to define trends among these different datasets until our analysis of the 2013 data is complete.

d. Marketing Contact via Mobile Phone

We also checked consumer understanding of the “rules of the road” for telemarketing via cell phones more generally. When a consumer gives her number to a person at a store’s till, does she understand the purpose? Telemarketing to wireless phones has been illegal since 1991, but firms may make sales calls to consumers with whom they have an established business relationship. This means that when a consumer gives contact information to a cashier, generally speaking, the business has established a relationship and can begin calling that consumer.

We explored both whether respondents understood this to be the case and their preferences about what the data usage rules *should* be. To do this, we asked respondents whether, if they provided their cell phone number to a cashier, the store should be able to call them later to offer more information about products and services. Seventy-four percent objected to this use of the cell phone number, an unsurprising result in light of the popularity of the Do Not Call Registry for objecting to telemarketing.¹²³ Twenty-four percent, however, agreed that the store should be able to call them. (Three percent did not know or did not respond.)

FIGURE 2: SHOULD A STORE BE ABLE TO CALL YOUR MOBILE PHONE?
(BASED ON ALL RESPONDENTS, $n=1203$)



Both the location-based tracking described above and mobile payments systems (such as those provided by Square, Google, and others) are likely to offer retailers the ability to engage in much more targeted marketing practices than they have previously been able to do—in theory, this could be quite useful to both consumers (who receive more relevant marketing) and businesses (whose ad budgets are focused on more targeted offerings).

123. As of December 2011, 209 million numbers have been enrolled in the National Do-Not-Call Registry. Press Release, Fed. Trade Comm’n, FTC Sends Biennial Report to Congress on the National Do Not Call Registry (Dec. 30, 2011), <http://www.ftc.gov/opa/2011/12/dnc.shtm>.

Payments systems may be particularly attractive in part because retailers presently receive very little information about the consumer when she pays for a purchase in a physical store with a credit card or cash. “Merchants are restricted in how they can collect data about consumers at the register, both through credit card acceptance agreements and by practical considerations.”¹²⁴ Mobile payments systems, however, can be configured to automatically convey unique consumer-identifying information to the retailer at the point of sale for later marketing or analytics use. As such, they may be attractive both for convenience and for information-gathering purposes.

Following our method of asking about actual new business practices, we asked respondents about their preferences for being identified to the merchant through mobile payments systems—specifically, whether they would be willing to have their phone number, email address, or postal mail address shared with retailers.

We found that 81%¹²⁵ objected to the transfer of their telephone number to a store where they purchase goods. Only 15% would “probably allow” such sharing, and 3% would “definitely allow” it.

Consumers’ home addresses seem to be just as sensitive as their telephone numbers. Eighty-one percent¹²⁶ said that they either definitely or probably would not allow sharing of their home address with a retailer. Similar to phone numbers, only 14% would “probably allow” such sharing, and 3% would “definitely allow” it.

While opposition to information sharing at the register is strong in all categories we analyzed, e-mail sharing seems to be the least sensitive category. Thirty-three percent would be willing or probably willing to share e-mail addresses at the register. Still, 51% stated that they would “definitely not allow” their e-mails to be shared, and 16% stated that they “probably would not allow” it.

III. DISCUSSION

A. *The More You Know: Converting Optimism and a Knowledge Gap into Pragmatism*

Like Westin, we found that “privacy pragmatists,” as defined by his segmentation, make up a stable category of survey respondents. Yet, when we probed their actual knowledge of privacy practices and protections, we found it limited, at best. Further, despite Westin’s

124. CHRIS JAY HOOFNAGLE ET AL., *MOBILE PAYMENTS: CONSUMER BENEFITS & NEW PRIVACY CONCERNS* 11 (2012), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045580.

125. Specifically, 65% stated that they would “definitely not allow” this sharing; 16% would “probably not allow” it.

126. Specifically, 66% stated that they would “definitely not allow” this sharing; 15% would “probably not allow” it.

prediction that data practices will follow pragmatists' preferences, we found high levels of rejection from all respondents, including pragmatists, when we presented them with relevant, real-world data collection practices and the business propositions those practices represent. These findings do not fit the Westin model. We think the reasons for the discrepancies can be found in Westin's survey methods and underlying assumptions.

Survey research can be a powerful, if limited, tool for evaluating theories, assumptions, and substantive coverage of privacy laws, as well as the default rules embedded in privacy law. But how it is employed is critical to its effectiveness. We explained in Part II that, descriptively, the assumptions that Westin employed to segment the public cannot properly be used to describe certain users as "pragmatic." More specifically, using our survey datasets, we show in Part II that the group of consumers Westin labeled "pragmatists" appears to act differently from the assumptions of the segmentation model in important ways. First, they appear to be operating in the marketplace under some important misconceptions about the default privacy protections in place. Second, they also appear to reject actual business models that, given the current and growing use of those models, they might be expected to have accepted if they play the role of market-defining "rational consumers" in today's marketplace.

These findings are consistent with one of the few academic critiques of Alan Westin's work, by Professor Oscar Gandy. In 1995, Gandy wrote,

The literature of communications effects provides quite compelling evidence that the indirect experience of others that we make use of when we read the papers, watch the news . . . influences our knowledge, attitudes, and opinions about the social world. When I examined some of the data that were gathered by Professor Westin and the Harris organization for an Equifax report in 1990, I discovered that the extent to which people had read or heard about "the potential use or misuse of computerized information about consumers" was a powerful explanatory factor. The more th[e]y had heard or read, the more they were concerned about threats to their privacy, the more concerned they were about the sale of personal information by list the industry. And consistent with a view that sees mediated experience as a source of social opinion, the more you heard or read, the less you trusted organizations that collected and used information about consumers.¹²⁷

127. Gandy, *supra* note 22 (internal citations omitted).

Gandy cautioned that Westin's recommendations for social policy omitted what Gandy referred to as "social research," especially a discussion of how power relationships between an individual, the state, and a business may affect privacy attitudes.¹²⁸

In his 1993 work *The Panoptic Sort*, Gandy noted that privacy concern is related to knowledge of marketplace activities.¹²⁹ He illustrated this by comparing individuals' existing concerns to their normative beliefs about business practices.¹³⁰ For instance, Gandy observed that in one survey, almost 40% of respondents thought that information sharing among businesses was something to be concerned about.¹³¹ However, 97% agreed that it was a "bad thing" that companies could buy information about consumer characteristics from mailing list companies.¹³² Under Gandy's approach, ignorance of business practices accounted for the gulf between the 97% who objected to information sharing and the much smaller group concerned about that practice.¹³³

128. *Id.* at 100, 102 ("Westin fails to use his tripartite division to good effect because he has not clearly identified the underlying tension that structures and is structured by changes in technology, social policy, and interpersonal relations. Westin's analysis fails to see, or if it sees, refuses to acknowledge, that the fundamental consideration is one of power.").

129. See OSCAR H. GANDY, JR., *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* 140-42 (1993). We note that the idea that privacy attitudes are related to knowledge is not a new one. In a colloquy between Guy Dobbs, then Vice President of Xerox Computer Services and member of a 1972 committee to review privacy issues, and Richard J. Gwyn, then Director General of the Department of Communication of the Government of Canada, the two discussed the disconnect between high privacy concern and the lack of complaints filed with officials concerning privacy violations. See Chris Jay Hoofnagle, *Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)*, BERKELEY L., <http://www.law.berkeley.edu/16452.htm> (last visited Apr. 5, 2014). Dobbs reasoned, "If . . . the populace does not realize and does not understand that, in fact, there are large amounts of data collected . . . if they literally do not understand that, then they have no basis . . . for arriving at a complaint." Guy Dobbs, Remarks at the Meeting of the Secretary's Advisory Committee on Automated Personal Data Systems 224 (Aug. 17, 1972), available at http://www.law.berkeley.edu/files/HEW/HEW_transcript_08171972.pdf. Richard J. Gwyn responded, "Evidently, there is a link between conditioning [and] the lack of knowledge of the individuals about their rights. In fact, in most cases, they do not have any rights that have been admitted by the organization; the organization simply asks for information and the individual gives it out expecting some how [sic] that the organization has some God-given authority to ask for it." Richard J. Gwyn, Remarks at the Meeting of the Secretary's Advisory Committee on Automated Personal Data Systems 224 (Aug. 17, 1972), available at http://www.law.berkeley.edu/files/HEW/HEW_transcript_08171972.pdf.

130. GANDY, *supra* note 129, at 142.

131. *Id.*

132. *Id.*

133. *Id.*

The core of Gandy's argument—that Westin failed to account for consumer knowledge in concluding that the public supported information sharing—was a critique used by the Federal Communications Commission (“FCC”) in deciding how to regulate the sale of individual calling records. The FCC argued that Westin, in writing a survey for PacTel, did not describe the kinds of information that that phone companies proposed to sell for marketing purposes—lists of the specific numbers called and received by consumers:

[T]he [Westin] survey questions ask broadly whether it is acceptable for a customer's local telephone company to look over “customer records” to determine which customers would benefit from hearing about new services, without explaining the specific types of information that would be accessed. Much CPNI [Customer Proprietary Network Information], however, consists of highly personal information, particularly relating to call destination, including the numbers subscribers call and from which they receive calls, as well as when and how frequently subscribers make their calls. This data can be translated into subscriber profiles containing information about the identities and whereabouts of subscribers' friends and relatives; which businesses subscribers patronize; when subscribers are likely to be home and/or awake; product and service preferences; how frequently and cost-effectively subscribers use their telecommunications services; and subscribers' social, medical, business, client, sales, organizational, and political telephone contacts.¹³⁴

Westin found consumer support for the selling of phone records by describing it without keying respondents into the actual practices and implications of them.¹³⁵ Consumers cannot have perfect knowledge of all business practices, nor would consumers find it efficient to acquire perfect knowledge.¹³⁶ But when answering questions in the PacTel study, consumers were kept in the dark about the key practice at issue.¹³⁷ Had they been given the basic information exchange to consider, consumers may have withdrawn their support.

134. Implementation of the Telecomms. Act of 1996: Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 13 FCC Rcd. 8061, 8107–08 (1998).

135. *Id.* at 8140. We note that these are the same kinds of records that are the subject of the telephone metadata program. See Ryan Lizza, *The Metadata Program in Eleven Documents*, NEW YORKER (Dec. 31, 2013), http://www.newyorker.com/online/blogs/comment/2013/12/a-history-of-the-metadata-program-in-eleven-documents.html#slide_ss_0=1.

136. *Implementation of the Telecomms. Act of 1996*, 13 FCC Rcd. at 8161–62.

137. *Id.* at 8140.

B. Reconceptualizing the Westin Framework: The Privacy Resilient, the Privacy Vulnerable, and Bargaining for Privacy

Viewed in a new light, Westin's segmentation may be seen as describing two groups, one with more accurate knowledge about business and legal protections and one with less. The more knowledgeable group is made up of Westin's privacy fundamentalists; this matches our knowledge-based findings. Beyond knowing more, this group is also more likely to engage in privacy self-help, according to Westin's own research.¹³⁸ We could think of these consumers as the "privacy resilient"—more knowledgeable and at least more willing to take steps to protect privacy.

The second group—made up of Westin's privacy pragmatists and unconcerned—labors in the marketplace with fundamentally misinformed views about privacy rules and a lower likelihood to take self-help measures. We could think of these consumers as the "privacy vulnerable"—less knowledgeable and less likely to take steps to protect privacy.

Despite their different abilities, both groups must operate in a marketplace where certain choices and sets of information are available and others are not. Recall that Westin thought public policy should be tailored to the pragmatists and that individual decisions made by consumers in the marketplace determine the success or failure of new technologies.¹³⁹

Rational choice theory is often misunderstood by critics as explaining individuals' preferences as rational and well-informed. Instead, the rational choice approach simply treats preferences as given—rational and informed or not—and predicts that consumers will act to maximize those preferences in the marketplace.¹⁴⁰ The rationality is focused on the pragmatic means that individuals use to maximize their own utility, not on the formation of their underlying preferences.¹⁴¹

138. See Westin, *supra* note 63. Overall, Westin found that 66% of respondents had engaged in four kinds of privacy-protective behaviors. Westin applied his privacy segmentation to the population, but did not use the fundamentalist/pragmatist/unconcerned labels; instead, he applied high/balanced/low concern labels. *Id.* Seventy-five percent of respondents with high privacy concern had taken at least four of the seven actions, and 65% of respondents with "balanced privacy concern" had taken at least four of the seven actions. *Id.* Among those who had "low privacy concern," 46% had taken at least four of the seven steps to protect privacy. *Id.*

139. *Id.*

140. See LAWRENCE E. BLUME & DAVID EASLEY, *THE NEW PALGRAVE DICTIONARY OF ECONOMICS* (Steven N. Durlauf & Lawrence E. Blume eds., 2d ed. 2008) (discussing the principle of rationality, which posits that individuals "act in their perceived best interests").

141. See *id.*

This misunderstanding is key to our critique. Westin's approach places a high value on individuals negotiating in the marketplace for privacy,¹⁴² but the knowledge gap we elucidate shows that many consumers both misunderstand the scope of data collection and already believe that relevant privacy rights are enshrined in privacy policies and guaranteed by law. And when presented with some typical current-day value propositions, high percentages reject them, even those made—and apparently accepted—every day in the marketplace. While we cannot draw a direct conclusion for the reason behind this mismatch, it plausibly indicates that myopia, created by lack of knowledge, is a contributing factor. Operating within this myopic view of their duties as consumers, individuals may find little reason to bargain for privacy in the marketplace.

Thinking in terms of myopia also addresses a common rational choice explanation that consumers do not read privacy policies because it is rational to remain ignorant. Simply put, this argument holds that it is not worth a consumer's time to learn about privacy issues. For instance, Professors Muris and Beales argue that

[t]he point is not that transaction costs are particularly high, because it does not take long to process a privacy notice. Rather, processing privacy notices is a cost that most consumers apparently do not believe is worth incurring. The perceived benefits are simply too low. . . . 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.¹⁴³

Leaving aside the actual (steep) transaction costs involved in reading privacy policies¹⁴⁴ and the fact that for many services—such

142. Westin, *supra* note 63.

143. J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 114 (2008).

144. Contrary to Beales and Muris' argument, the transaction costs associated with reading privacy policies are quite high. Taken seriously, the argument that individuals should read privacy policies for all the sites they visit would mean that Internet users would spend more time reading privacy notices than much of the content they were seeking. A longitudinal study of privacy policies found that they are written above a high school reading level, that they are becoming more difficult to read, and that they are becoming longer (on average, 1,951 words each). See George R. Milne et al., *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MARKETING 238, 242–43 (2006). McDonald and Cranor showed in 2008 that if consumers read all the first-party privacy policies on sites they visit, it would come at a \$781 billion opportunity cost. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 564 (2008). "[I]n considering ex ante search costs of consumers comparing

as mobile apps or passive location tracking—policies may be hard to find or nonexistent, our approach frames this conundrum differently. It is not that people do not care. It is that they often do not understand the exchange involved, and they think that they are protected in any event, and so they do not believe there is value to be had in reading about those protections. Why would one stop to read an eight-page-long policy if she believed that she already knew what practices it described and what rights it conferred?

To the extent that large numbers of consumers are unaware of privacy problems and the need to protect themselves in the marketplace, privacy is a less marketable value. The Westin approach distorts the market for privacy because the system leaves aside the reality of a marketplace where the consumer decision maker does not understand material aspects of the bargain and assumes that aspects of interest are already decided in her favor.

Westin's focus on "privacy pragmatists" as the deciding cohort leaves the least knowledgeable consumers without protection in the marketplace. Further, these consumers' deficits prevent them from realizing that it is their duty to negotiate for privacy. As noted in Part I, we agree that marketplace adoption can determine its success in marketplace. This makes it all the more necessary to address consumer knowledge gaps and optimism about the protections they are afforded by business practices and the law. If unaddressed, invasive business models will become the norm, despite consumer preference for more protection. With ever-increasing data collection and tailoring, this is timely and growing concern.

CONCLUSION

Professor Westin's privacy segmentation is a well-known and broadly applied framework for understanding privacy attitudes and consumer choices in the marketplace. It presents a romantic and positive view of consumers—one that sees them as individual, rational, and deliberative actors who, through their individual marketplace decisions, have collective effects on business models. Using this lens, Westin's ideal for privacy regulation was a system where a pragmatic *homo economicus* protected himself in the marketplace.

However, Westin's privacy segmentation model labels a broad group of American consumers as "pragmatists" without establishing

different services, the consumer may have to read the equivalent of eight pages of materials per competitor just to evaluate privacy issues." Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327, 1358 (2012) (discussing the ex ante transaction costs elucidated by the research of McDonald, Cranor, and Milne et al.); see generally Melvin Aron Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 STAN. L. REV. 211 (1995).

whether they actually engage in the kind of deliberations that define pragmatism. Further, our empirical research supports and goes beyond more general experimental work to reveal that many consumers negotiate privacy preferences based on fundamental misunderstandings about business practices, privacy protections, and restrictions upon the use of data, and that these misunderstandings may lead them to expect more protection than actually exists. When presented with specific information privacy propositions actually offered in the marketplace, most prefer more control than they are presently afforded. These misunderstandings distort the market for privacy because they cause consumers to believe that they need not negotiate for privacy protections.

Overall, our findings show that many individuals' decisions are deeply misinformed about business practices and legal protections, and that Westin "pragmatists" understand less than either "fundamentalists" or the "unconcerned." Finally, when given real-world scenarios that surface the privacy tussle present in new services, we find that pragmatists, contrary to Westin's description, join fundamentalists in rejecting information-intensive service options.

Thus, the most cited aspect of Westin's work—his characterization of consumers' decisions as pragmatic, and his argument that consumer decisions signaled the collective sense of how society should balance privacy and new technologies—should, we think, be strongly questioned. Westin's approach attached a euphemistic "super-consumer" label to users' decisions. It confused deliberate choice with the reality that most consumers must accept the business models that are available to them. Conceptualizing users as super-consumers distorts our understanding of the market for privacy and places the blame for the spread of privacy-invasive services at the feet of consumers. This focuses the policy debate on the consumer rather than on the structures of the marketplace.

The influence of the segmentation model and rational choice in the privacy marketplace should be revisited. We should devise methods that give us more accurate pictures of consumer knowledge and preferences, and apply them to develop effective policy. A more responsive and effective system of consumer protection would create incentives to close the knowledge gap consumers experience and better connect individuals' expectations for legal protections with reality. Instead, consumers are left in the dark in making marketplace decisions that, ultimately, affect which technological services are socially acceptable and which are not.

But we also think it would be a shame for Professor Westin's seminal work on privacy to be diminished as the assumptions behind the segmentation model fade. Rather, our focus should shift to his fundamental argument that it is humans espousing and employing privacy as a liberal value—not technological capacity or bare business preferences—who can and should make decisions

about information flows and data privacy as machine information processing gets ever more sophisticated. Westin's understanding of humans operating as *homines economici* when making privacy decisions has been eclipsed by a richer understanding of human behavior and preferences, but his call for society to make these decisions decidedly has not.

Privacy and Freedom has unfortunately fallen out of print; indeed, it is relatively difficult and expensive to obtain even a used copy in today's marketplace.¹⁴⁵ Perhaps it is time to revive this classic text, and revisit its lessons in the context of today's privacy challenges.

145. As of this writing, Amazon.com hosted 14 offers—just about enough for one small seminar—for used copies of *PRIVACY AND FREEDOM*, ranging from about \$40.00 for a copy in “good” condition to about \$120.00 for a copy in “very good” condition. See *Used Offers for “Privacy and Freedom” (Hardcover)*, AMAZON, http://www.amazon.com/gp/offer-listing/0689102895/sr=8-1/qid=1395102321/ref=olp_page_next?ie=UTF8&colid=&coliid=&condition=used&me=&qid=1395102321&shipPromoFilter=0&sort=sip&sr=8-1&startIndex=10 (last visited Mar. 17, 2014).

APPENDIX A: 2009 SURVEY RESEARCH FINDINGS (N=1,000)

	(%)
<i>Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?</i>	
Yes, there should be a law	69
No, a law is not necessary	29
DK	2
<i>Do you think there should be a law that requires websites and advertising companies to delete all stored information about an individual, if requested to do so.</i>	
Yes, there should be a law	92
No, a law is not necessary	7
DK	1
<i>Advertisers would like to keep and store information about your internet activity. How long should they be able to keep it? Do you think—</i>	
They should have to delete it immediately, OR	63
They should be allowed to keep it for a few months, OR	25
They should be allowed to keep it for a year, OR	6
They should be allowed to keep it for as long as they want	4
DK	2
<i>If a company purchases or uses someone's information illegally, about how much—if anything—do you think that company should be fined?</i>	
\$100	2
\$500	4
\$1,000	9
\$2,500	7
More than \$2,500	70
It depends	4
DK	4
<i>Beyond a fine, companies that use a person's information illegally might be punished in other ways. Which one of the following ways to punish companies do you think is most important?</i>	
The company should fund efforts to help people protect privacy	38
Executives who are responsible should face jail time	35
The company should be put out of business	18
The company should not be published in any of these ways	3
It depends	2
DK	4

Compared to five years ago, would you say you are more concerned about privacy issues on the internet, less concerned, or that you have about the same level of concern?

	<i>02/12</i>	<i>07/09</i>
More concerned	66	55
Less concerned	5	6
Same level	28	38
Don't know/Refused	1	1
	<i>N=1,203</i>	<i>N=1,000</i>

Please tell me which ONE of the following is the MOST important reason you are more concerned about privacy issues on the internet than you were five years ago . . .

	<u>2/12</u>	<u>7/09</u>
You know more about privacy risks online (or)	47	49
You have more to lose if your privacy were violated (or)	33	29
You have had an experience that has changed your mind about privacy (or)	16	17
(DO NOT READ) Some other reason? (SPECIFY)	2	3
Don't know/Refused	2	2
	(n=818)	(n=563)

When using the internet, do you erase your cookies . . . (READ)

Often	40
Sometimes	23
Hardly ever	16
Never	12
(Vol.) Not familiar with cookies	6
(Do not read) Don't know/Refused	3

Do you read the privacy policies of websites . . . (READ)

Often	14
Sometimes	36
Hardly Ever	31
Never	18
(Do not read) Don't know/Refused	1

Have you ever changed your mind about buying something online because of a privacy or security concern?

Yes, have	56
No, have not	38
(Do not read) Does not shop online	6
Don't know/Refused	*

In general, how often do you check your credit report—at least once a month, every few months, about once a year, less than once a year, or never?

At least once a month	10
Every few months (quarterly)	18
About once a year	34
Less often than once a year	18
Never	19
Don't know/Refused	1

AMERICANS' KNOWLEDGE OF LAWS ONLINE AND OFFLINE 2009
 (N=1,000)
 (FOR EACH STATEMENT, FALSE IS THE CORRECT ANSWER)

	False (%)	True (%)	DK (%)
Online			
If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.	22	62	16
If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government.	46	26	28
If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so.	20	54	26
If a website violates its privacy policy, it means that you have the right to sue the website for violating it.	19	46	35
If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission.	48	33	19
Offline			
When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission.	49	36	15
When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission.	31	44	25
When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission.	57	28	15
When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission.	33	49	18

APPENDIX B: 2012 SURVEY RESEARCH FINDINGS (N=1,203)

Some people think there should be a system like the National Do Not Call list that would help reduce the amount of advertisements you receive in your postal mailbox. Would you strongly support, support, oppose, or strongly oppose the creation of such a system?

43	Strongly support
38	Support
12	Oppose
5	Strongly oppose
2	Don't know/Refused

I am going to read a list of statements about online privacy policies. As I read each one, please tell me whether you think it is true or false, to the best of your knowledge. If you're not sure of an answer, just tell me, and we'll go to the next item. (First,) what about this statement . . . (What about (INSERT NEXT ITEM) . . .

Do you think this statement is true or false, or do you not know?

	True (%)	False (%)	DK (%)	Ref. (%)
When you use the internet to learn about medical conditions, advertisers are not allowed to track you in order to target advertisements	22	36	41	1
Free websites that are supported by advertising are allowed to sell information gathered from users of the site, even if they have a privacy policy	40	19	40	*
When visiting free websites supported by advertising, you have the right to require the website to delete the information it has about you	25	32	42	*

In general, how often do you find online advertising, such as the advertising that appears on search results webpages and banner advertisements, useful?

10	Often
20	Sometimes
36	Hardly ever, OR
33	Never?
1	Don't know/Refused

How often do you click on advertisements when using the internet?

2	Often
12	Sometimes
35	Hardly ever, OR
50	Never?
*	Don't know/Refused

When you use a free website, one that is supported by advertising, do you have more privacy rights, less privacy rights, or about the same amount of rights as when you use a website that charges a fee for its use?

2	More rights
40	Less rights
36	About the same amount
22	Don't know/Refused

Compared to five years ago, would you say you are more concerned about privacy issues on the internet, less concerned, or that you have about the same level of concern?

	<u>2/12</u>	<u>7/09</u>
More concerned	66	55
Less concerned	5	6
Same level	28	38
Don't know/Refused	1	1
	<i>N</i> =1,203	<i>N</i> =1,000

Please tell me which ONE of the following is the MOST important reason you are more concerned about privacy issues on the internet than you were five years ago . . .

	<u>2/12</u>	<u>7/09</u>
You know more about privacy risks online (or)	47	49
You have more to lose if your privacy were violated (or)	33	29
You have had an experience that has changed your mind about privacy (or)	16	17
(DO NOT READ) Some other reason? (SPECIFY)	2	3
Don't know/Refused	2	2
	(<i>n</i> =818)	(<i>n</i> =563)

Are you more concerned about the collection and use of information by the government, by private companies, or by both the government and private companies? (*N*=1,203)

11	Government (or)
19	Private companies (or)
66	Both the government and private companies (or)
2	(VOL.) Neither
2	Don't know/Refused

Cell phone service providers can track the location of all the cellphones on their networks. This location information is highly accurate and available even when the subscriber is NOT making a call.

How long should cellphone service providers keep information about subscribers' location?

	<u>8/13</u>	<u>2/12</u>
Less than a year	29	28
One to two years	17	9
Two to five years	7	6
Indefinitely	10	7
Or should they not be able to keep it?	33	46
(DO NOT READ) Don't know/Refused	3	4
	(n=923)	(n=1119)

Some cell phone service providers are considering using information about subscribers' location in order to tailor advertisements to the subscriber. Would you definitely allow, probably allow, probably not allow, or definitely not allow your cellphone service provider to use information about your location to tailor advertisements to you?

	<u>8/13</u>	<u>2/12</u>
Definitely allow	4	1
Probably allow	11	7
Probably not allow	17	22
Definitely not allow	66	70
Don't know/Refused	2	1
	(n=923)	(n=1119)

If you provide your wireless or cell phone number to a cashier, should the store be able to call you later to provide information about other products or services that the store offers?

24	Yes, they should be able to call
74	No, they should not call
3	Don't know/Refused

Some social networking apps, such as Facebook, may collect the contact list information stored on your phone in order to suggest more connections/friends to you. Would you definitely allow, probably allow, probably NOT allow, or definitely NOT allow an app to do this? *Based on cell phone owners (n=1119)*

4	Definitely allow
14	Probably allow
30	Probably not allow
51	Definitely not allow
2	Don't know/ Refused

Now imagine that you just downloaded a coupons app. This app helps you find coupons when you are out shopping. The app can also send people listed in your phone's contact list coupons. In order to do so, this app needs to read your contacts list on your phone. Would you definitely allow, probably allow, probably not allow, or definitely not allow this coupons app to read your contacts list? *Based on cell phone owners (n=1119)*

2	Definitely allow
4	Probably allow
18	Probably not allow
75	Definitely not allow
1	Don't know/ Refused

If you decided to start using your cell phone to pay for items, would you definitely allow, probably allow, probably NOT allow, or definitely NOT allow this service to (INSERT. READ AND RANDOMIZE ITEMS B-D). What about (INSERT NEXT ITEM)? *Based on cell phone owners (n=1119)*

	Definitely allow	Probably allow	Probably not allow	Definitely not allow	Don't know/ Refused
<i>Share information about you with the stores you visit, when you are just browsing</i>	1	3	17	79	*
<i>Share your number with the stores where you make purchases</i>	3	15	16	65	*
<i>Share your email address with the stores where you make purchases</i>	6	27	16	51	1
<i>Share your home address with the stores where you make purchases</i>	4	14	15	66	1

APPENDIX C: 2013 SURVEY RESEARCH FINDINGS

Berkeley Trend Information

11/13: University of California—Berkeley. PSRAI November Omnibus Survey (November 7–10, 2013). 1,003 adults. MOE +/-3 percentage points.

9/13: University of California—Berkeley. PSRAI September Omnibus Survey (September 25–29, 2013). 1,005 adults. MOE +/-3 percentage points.

8/13: University of California—Berkeley. PSRAI August Omnibus Survey (August 8–11, 2013). 1,002 adults. MOE +/-3 percentage points.

Please tell me if you strongly agree, agree, disagree, or strongly disagree with these statements.

	<u>11/13</u>	<u>9/13</u>	<u>8/13</u>
<i>Consumers have lost all control over how personal information is collected and used by companies.</i>			
Strongly agree	23	28	25
Agree	42	40	47
Disagree	27	24	22
Strongly disagree	4	4	4
DK/Ref.	4	3	3
<i>Most businesses handle the personal information they collect about consumers in a proper and confidential way</i>			
Strongly agree	5	8	8
Agree	47	46	48
Disagree	32	30	31
Strongly disagree	11	11	10
DK/Ref.	4	4	4
<i>Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.</i>			
Strongly agree	4	6	6
Agree	43	40	48
Disagree	36	36	31
Strongly disagree	13	12	12
DK/Ref.	5	5	3

Compared to five years ago, would you say you are more concerned about privacy issues on the internet, less concerned, or that you have about the same level of concern?

	<u>11/13</u>	<u>9/13</u>	<u>8/13</u>
More concerned	62	62	63
Less concerned	4	5	4
Same level	32	31	30
Don't know/ Refused	2	2	3

Please tell me which ONE of the following is the MOST important reason you are more concerned about privacy issues on the internet than you were five years ago . . .

	<u>11/13</u>	<u>9/13</u>	<u>8/13</u>
You know more about privacy risks online (or)	40	47	43
You have more to lose if your privacy were violated (or)	26	27	23
You have had an experience that has changed your mind about privacy (or)	16	12	17
(DO NOT READ) Some other reason?	14	13	12
Don't know/Refused	4	2	6
	(n=624)	(n=624)	(n=625)

Are you more concerned about the collection and use of information by the government, by private companies, or by both the government and private companies?

	<u>11/13</u>	<u>9/13</u>	<u>8/13</u>
Government (or)	13	16	13
Private companies (or)	14	15	14
Both the government and private companies (or)	66	63	65
(VOL.) Neither	5	4	6
Don't know/Refused	2	2	2

Do you use the internet at least occasionally?

	<u>11/13</u>	<u>9/13</u>	<u>8/13</u>
Yes	84	85	86
No	16	15	14
Don't know/Refused	*	*	*

Cell phone service providers can track the location of all the cellphones on their networks. This location information is highly accurate and available even when the subscriber is NOT making a call.

How long should cellphone service providers keep information about subscribers' location?

	<u>8/13</u>	<u>2/12</u>
Less than a year	29	28
One to two years	17	9
Two to five years	7	6
Indefinitely	10	7
Or should they not be able to keep it?	33	46
(DO NOT READ) Don't know/Refused	3	4
	(n=923)	(n=1119)

Some cell phone service providers are considering using information about subscribers' location in order to tailor advertisements to the subscriber. Would you definitely allow, probably allow, probably not allow, or definitely not allow your cellphone service provider to use information about your location to tailor advertisements to you?

	<u>8/13</u>	<u>2/12</u>
Definitely allow	4	1
Probably allow	11	7
Probably not allow	17	22
Definitely not allow	66	70
Don't know/Refused	2	1
	(n=923)	(n=1119)

Would you definitely allow, probably allow, probably NOT allow, or definitely NOT allow your cell phone provider or apps on your phone to share information about you with the stores that you visit while you are out shopping? [READ AS NECESSARY: Would you definitely allow, probably allow, probably NOT allow, or definitely NOT allow this?]

	<u>8/13</u>
Definitely allow	2
Probably allow	9
Probably not allow	18
Definitely not allow	70
Don't know/Refused	1
