

The Privacy Pragmatic as Privacy Vulnerable

Jennifer M. Urban & Chris Jay Hoofnagle
University of California, Berkeley School of Law
Berkeley, CA 94720
jurban, choofnagle [@law.berkeley.edu]

ABSTRACT

Alan Westin's well-known and often-used privacy segmentation fails to describe privacy markets or consumer choices accurately. The segmentation divides survey respondents into "privacy fundamentalists," "privacy pragmatists," and the "privacy unconcerned." It describes the average consumer as a "privacy pragmatic" who influences market offerings by weighing the costs and benefits of services and making choices consistent with his or her privacy preferences. Yet, Westin's segmentation methods cannot establish that users are pragmatic in theory or in practice. Textual analysis reveals that the segmentation fails theoretically. Original survey data suggests that, in practice, most consumers are not aware of privacy rules and practices, and make decisions in the marketplace with a flawed, yet optimistic, perception of protections. Instead of acting as "privacy pragmatists," consumers experience a marketplace myopia that causes them to believe that they need not engage in privacy analysis of products and services. Westin's work has been used to justify a regulatory system where the burden of taking action to protect privacy rests on the very individuals who think it is already protected strongly by law. Our findings begin to suggest reasons behind both the growth of some information-intensive marketplace activities and some prominent examples of consumer backlash. Based on knowledge-testing and attitudinal survey work, we suggest that Westin's approach actually segments two recognizable privacy groups: the "privacy resilient" and the "privacy vulnerable." We then trace the contours of a more usable segmentation and consider whether privacy segmentations contribute usefully to political discourse on privacy.

1. INTRODUCTION

Professor Alan Furman Westin (1929-2013) advised on over 100 consumer surveys in his illustrious career. His well-known privacy segmentation is widely used in various fields.

Although Westin was also a preeminent historian and scholar of privacy law, his survey research sprang from his role as a consultant to information-intensive firms.^[7] As a result, he generally did not publish it academically. Given this, it has been subject to only a few sustained analyses, which appear to have gone unanswered by Westin.^[3,4,6]

In this position paper, we describe the Westin privacy segmentation, offer a textual analysis, and present empirical data that both call into question longstanding assumptions used by Westin and lend new insight into consumers' privacy knowledge and preferences.

Westin's tripartite segmentation interpreted individuals' marketplace privacy choices as knowing and deliberate. In our narrative, this is not the case. Instead, most consumers have substantial deficits in their knowledge of privacy law and of business practices. They do not, as Westin argued, "weigh the potential pros and cons of sharing information, evaluate the protections that are in place and their trust in the company or

organization . . . [and then] decide whether it makes sense for them to share their personal information."^[10] Our counter-narrative explains why consumers so often are surprised by information practices exposed in the media—they think these practices are illegal. Westin's explanation of consumer behavior has lent great support to opt-out approaches and self-regulatory regimes; this counter-narrative calls some of these approaches into question.

After discussing the Westin segmentation, we trace the contours of improved segmentations, and then discuss whether such segmentations have practical utility in the political sphere.

In part, this position paper is a shortened version of our forthcoming article, *Alan Westin's Privacy Homo Economicus*, 48 WAKE FOREST LAW REVIEW ____ (2014), available at <http://papers.ssrn.com/abstract=2434800>. Sections 4.1 and 4.2, which trace a new segmentation model and discuss the utility of segmentations generally, are new.

2. THE WESTIN 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). For many years, academics from a variety of disciplines have used the Westin segmentation for privacy analysis. For example, it has recently been employed in psychology, in the study of marketing, in computer security, and in the information and communications technology contexts. Beyond the academy, the segmentation has notably influenced United States privacy regulation by undergirding the predominant "notice and choice" regime, under which consumers, given information about privacy trade-offs, are expected to choose products and services according to their preferences. In many ways, the "notice and choice" model assumes that consumers will act as "privacy pragmatists," and that the privacy fundamentalists' preferences are powerful enough to police the marketplace and influence less-involved consumers.

In 2002 Westin made the clearest extant summary of the 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. . . .

"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.[10]

3. CRITIQUE OF THE WESTIN SEGMENTATION

3.1 The segmentation instrument does not establish that individuals are pragmatic in theory or in practice

Our first critique focuses on the methods Westin used to categorize consumers as fundamentalists, pragmatists, or unconcerned. Ponnurangam Kumaraguru and Lorrie Cranor have engaged in the most careful review of Westin's privacy segmentation. They found that Westin generally asked respondents these three questions:

“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.

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.[6]

It thus appears that Westin coded privacy pragmatists as the default category—“all other respondents.” This is problematic as a matter of logic because pragmatism 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.¹ 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, nor do they accurately capture fundamentalism or unconcern. For example, 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 yet 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.

Because of these instrumental deficits, it is not possible to answer Westin's screening questions and come to the conclusion that the proposed groups exist, much less 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, they decide whether it makes sense for them to share their personal information.”[10]

Accordingly, the Westin segmentation cannot establish any group as “pragmatists.” It could be that Westin used other questions from his surveys to establish the link to pragmatism, but this is not apparent from his extant surveys. Westin generally did not publish his work academically and did not explain any method he might have used in moving from the segmentation to the segment descriptions.

We next turn to two empirical critiques based on two surveys on privacy knowledge and issues. Both polls were national, telephonic (landline and wireless) surveys. The 2009 study surveyed 1,000 Internet users, and the 2012 study surveyed 1,203. Fuller results and survey instruments are available in our longer *Privacy Homo Economicus* paper and at: <http://www.law.berkeley.edu/privacysurvey.htm>.

3.2 A knowledge gap causes Americans to falsely believe that privacy policies mandate strong legal protection

In both surveys, respondents appeared 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

¹ We do not object in principle to the composition of Guttman scales and the idea of default categories generally. Our point concerns the special characteristics of being a “pragmatist,” which requires a series of active behaviors and decisions. People are not pragmatic by default.

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." [8,9]

The 2009 survey included a quiz that explored respondents' knowledge about the 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." 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.

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. Complicating narratives about "digital natives," younger respondents did most poorly, with 42% answering none of the online questions correctly, and 50% answering none of the offline questions correctly.

3.2.1 Privacy pragmatists are less knowledgeable than people in other segments

In 2012, we again asked questions that tested respondents' knowledge about privacy protections in the marketplace. Privacy fundamentalists answered all three knowledge questions correctly in greater proportion than the other groups; all such differences between groups were significant at a p of .01 or better. 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. 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.

3.2.2 Privacy pragmatists' knowledge deficits preclude true pragmatic action in the marketplace

Westin presents the privacy pragmatist as a "super consumer," evaluating the benefits and risks of technology in a rational choice theory framework. However, our work shows that pragmatists' knowledge gap would affect this key behavior. If pragmatists believe that privacy policies create privacy protections, then they do not understand that it is their duty to read and compare privacy policies, evaluate them for fair information practices, compare marketplace offerings according to their protections, and so on. The knowledge gap makes pragmatic action as described by Westin unlikely to occur.

3.3 When respondents were confronted directly with examples of extant marketplace information collection and use, they expressed preferences contrary to Westin's predictions

In our 2012 survey, we asked Americans about a variety of real-world collection and uses of mobile phone data, a rapidly growing sector of information-rich tracking and marketing. Our instrument used these real-world scenarios to surface the marketplace exchange being offered (usually information collection and use in return for a consumer benefit). These details of such exchanges are often hidden to consumers, who may only be told that a service is "free." The Westin model predicts that the average consumer, a privacy pragmatist, would investigate these hidden factors, weigh them against the benefit of the exchange, and in the process evaluate whether the company was trustworthy and following fair information practices.

We found that instead, large numbers of respondents categorically rejected several forms of information-intensive activities that exchange data collection for some consumer benefit. These included: gathering contact list information from phones to provide suggestions for new social networking connections or coupons to friends (with 75% choosing "definitely not allow"), the use of presence-sensing technology to identify the consumer in a store (with 70% choosing "definitely not allow"), and location-based ad targeting (with 70% choosing "definitely not allow"). These models were broadly rejected, including by privacy pragmatists. In their real-world applications, the scenarios have in some cases prompted consumer backlash in the market.

4. DISCUSSION

Viewed in a new light, Westin's segmentation can 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. 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 is less likely 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.

Westin's approach places a high value on individuals negotiating in the marketplace for privacy, but the knowledge gap we elucidate shows that many consumers both misunderstand the scope of data collection and falsely believe that relevant privacy rights are enshrined in privacy policies and guaranteed by law. Further, 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 theory 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.[2] We suggest that it may not be that people do not care. Instead, it is more likely that they often do not understand the exchange involved, and think 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?

If large numbers of consumers do not understand the *quid pro quo* exchange being offered when information is collected or used or hold inaccurate beliefs about privacy protections in the marketplace, then privacy is a less marketable value. Employing the Westin segmentation distorts the market for privacy, because it 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.

4.1 Contours of an improved segmentation

Our findings suggest that the Westin segmentation, and its use to inform both marketplace offerings and privacy policy, are flawed. A more usable segmentation requires at least the following characteristics:

- It should adequately measure the information about privacy preferences that is required for a specific purpose. For example, a marketing purpose may require a different tool from a policy-making purpose.
- It should recognize that privacy is a nuanced issue, and that individuals react differently to different actors. For instance, it is well established that most Americans are concerned about both government and business data practices, but some are only concerned about the state, and others, only about the private sector.
- It should also recognize that individuals may respond differently to different *actions*. For instance, many people conceive of privacy as “access to the self,” and perceive events such as a telemarketing call or spam as a privacy problem. A consumer who holds such a conception may reject calls and spam, but overlook the collection and uses of data that made the telemarketing call or spam possible (or, to add more complexity, the use of information to decide not to call or email).
- It should logically segment groups based on an objective instrument that avoids the line-drawing issues the Westin segmentation exhibits. Building such an instrument requires work beyond this paper. However, questions that objectively test knowledge rather than attitudes could be a useful component.
- It should accurately portray salient group characteristics. Because privacy is a nuanced topic and is interpreted in many ways, a usable segmentation should accommodate multiple factors about an individual. Factors that, in our estimation, could shape privacy attitudes include: knowledge about privacy protections or business practices; how often the

respondent hears about privacy controversies in the news; whether the individual has had a bad experience relevant to privacy issues, such as identity theft, stalking, or an intractably error-ridden credit report; race; gender; socioeconomic class; and attitudes toward government and law enforcement.

- Its accuracy and reliability should be testable, and should show validity over time. Testing should include replication of the findings rather than simple market uptake of a product or service. This is necessary to accommodate the problem that the market is often not a good test bed for privacy attitudes. For instance, the market may reflect the knowledge gap we describe, or may provide no privacy-protective choice for services, or choices that are misunderstood or symbolic (such as the Online Behavioral Advertising opt out options). We note that survey research is limited in this dimension because respondents may feel judged for providing certain responses (such as revealing that they do not shred sensitive mail).
- It should accurately reflect the marketplace. If it measures preferences about business propositions being made in the marketplace, all relevant components of the choice should be clear to the respondent. For example, if a product is offered in exchange for personal information rather than money, the question should neutrally provide details about that exchange, rather than simply saying that the product is offered “free.”
- So far as possible, it should be based on measurements (such as privacy knowledge) that can be stably repeated over time to allow a baseline to be established and changes in responses to be measured.
- It should segment groups into categories that can accurately inform policy makers of the interests at stake when crafting policy compromises, such as groups that might warrant greater or lower levels of protection.

Based on this, we propose that the “privacy vulnerable” and “privacy resilient” groups drawn from our knowledge and attitude instruments are more usable segmentation categories than the tripartite Westin categories. That said, there is further work to be done in order to understand whether our categories are more usable and whether they meet the criteria listed in this section. Indeed, as we discuss next, we think there is more work to be done to decide whether segmentation models are useful, at all.

4.2 Utility of segmentation models

Section 4.1 sets forth contours for a better segmentation. It is immediately apparent that a lot of work needs to be done to improve segmentation models. This raises a serious question: what is the utility of segmentation models, overall? Is the game worth the candle?

One might want a segmentation to determine whether information collection and use should be opt-in (data subject must affirmatively accept) or opt-out (data subject must affirmatively reject). For instance, the Telemarketing Sales Rule requires the consumer to take action to avoid telemarketing. The overwhelming majority of Americans have taken this action, suggesting that they rejected the benefits (more marketing offers) offered in the exchange for additional privacy protection. Perhaps

it would have made sense to flip the default rule so that the great majority of individuals did not have to take affirmative action to reject telemarketing. But one does not need a segmentation to make that determination.

Similarly, one might want a segmentation that can reveal societal groups who are especially vulnerable to some privacy-related harms, because they are less knowledgeable, limited in the choices they can make, more vulnerable to consequences, or for some other reason.[1,10] Such groups might warrant different types of regulatory protection, benefit from additional information, and the like.

We suspect that Westin's segmentation was developed for different purposes—marketing strategy purposes—and then later applied as a political tool. If the segmentation were more accurate, businesses could use the segmentation testing to identify those who would not need to be sold on a product (the unconcerned), those who would not buy under any circumstance (the fundamentalist), and a large middle group that would be open to purchasing a product and would merely need to be informed about it in order to buy. Such a segmentation would allow a business to target its advertising investments. Since business information need only be good enough to improve sales, Westin's formula could have been valuable for marketers, despite its flaws.

The use of Westin's segmentation in the political realm was problematic, however. Many of Westin's surveys were funded by private companies and ratified these companies' public policy goals. The tripartite segmentation allowed them to divide the public into thirds and combine two of the groups to come to a favored conclusion.

More generally, we question the utility of segmentation because, at present, privacy law treats all individuals equally. The privacy unconcerned receives the same treatment as the fundamentalist.

At the workshop, we would like to explore with other participants whether and how segmentations are valuable, and whether they have utility in legal considerations of privacy.

5. CONCLUSION

Westin's privacy segmentation model labels a broad group of American consumers as "pragmatists" without establishing whether they actually engage in the kind of deliberations that define pragmatism. 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. Further, when presented with specific information privacy propositions actually offered in the marketplace, most respondents preferred 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.

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, and focuses the policy debate on consumer behavior, without considering the marketplace's structural influences.

This pragmatic "super-consumer" model is reflected in the much-used segmentation Westin employed in his survey research. Our textual review and empirical testing show that Westin's segmentation method exhibits fundamental flaws. A new segmentation method is required if segmenting consumers is to become a more usable tool. While we propose some requirements for a most accurate and useful segmentation method, we leave open the question of whether segmentation offers sufficient information about consumer privacy to be pursued at all.

6. REFERENCES

- [1] Allen, Anita, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011).
- [2] Beales, J. Howard, III & Muris, Timothy J., *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109 (2008).
- [3] Gandy, Oscar H. Jr., *Public Opinion Surveys and the Formation of Privacy Policy*, 59 J. Soc. Issues 283 (2003)
- [4] Gandy, Oscar H. Jr., *The Role of Theory in the Policy Process: A Response to Professor Westin*, in TOWARD AN INFORMATION BILL OF RIGHTS AND RESPONSIBILITIES (Charles M. Firestone & Jorge Reina Schement eds., 1995).
- [5] Katz, James E. & Tassone, Annette R. *Public Opinion Trends: Privacy and Information Technology*, 54 Pub. Opinion Q. 125 (1990).
- [6] Kumaraguru, Ponnurangam & Cranor, Lorrie Faith, *Privacy Indexes: A Survey of Westin's Studies* (2005), <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf>.
- [7] Simpson, Glenn, *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..").
- [8] Turow, Joseph, *Americans & Online Privacy: The System is Broken* (2003), http://editor.annenbergpublicpolicycenter.org/wp-content/uploads/20030701_online_privacy_report2.pdf;
- [9] Turow, Joseph et al., *Open to Exploitation: American Shoppers Online and Offline* (2005) http://editor.annenbergpublicpolicycenter.org/wp-content/uploads/Turow_APPC_Report_WEB_FINAL2.pdf.
- [10] Westin, Alan F. Harris Interactive, *Privacy On and Off the Internet: What Consumers Want* (2002) <http://www.ijsselsteijn.nl/slides/Harris.pdf>.

Copyright is held by the authors. Permission to make digital or hard copies of all or part of this work for noncommercial personal, research, or classroom use, with attribution, is granted without fee.

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA.