THE EYE OF THE BEHOLDER

OPERATIONALIZING **PRIVACY** BY DESIGN THROUGH THE POWER OF **CONSUMER CHOICE**

AUTHORS

Andrew Serwin, Esq.
CIPP/E, CIPP/U.S., CIPP/G.

Tina Stow, MA, CIPP

DATE PUBLISHED

July 2012

THE LARES INSTITUTE

APCO worldwide®

TABLE OF CONTENTS

To jump to a particular section, click on your desired section title below.
To return to this page, click on the ⏮ symbol at the top of the page.

3 About the Authors

4 Executive Summary

5 Introduction

7 Privacy is a Subjective Issue That is Currently Undefined

9 Timeline of Privacy Models, Key FTC Events and Proportionality

12 Privacy, Subjectivity and Proportionality

13 Data Elements and Data Sensitivity Rankings

16 Understanding Privacy Sensitivity

17 Self-Identified Sensitivity and Data-Element Sensitivity

19 Demographics and Data-Element Sensitivity

20 Conclusion

21 A Description of the Study

22 Endnotes

ABOUT THE AUTHORS

Andrew Serwin is the executive director and CEO of the Lares Institute and the founding chair of Foley & Lardner LLP's privacy practice. He is an internationally recognized thought leader regarding information and its role in the global economy and has handled leading matters before the Federal Trade Commission in information security, COPPA, social media, endorsement guidance and the sale of internet information.

He was named to *Security Magazine's* "25 Most Influential Industry Thought Leaders" for 2009, was ranked second in the most recent *Computerworld* survey of top global privacy advisors, is recognized by *Chambers USA* as one of the top privacy and data security attorneys nationwide (2009-2012) and was selected for inclusion in the *San Diego Super Lawyers®* lists (2007-2012), including being ranked in the Top 50 lawyers in 2012.

He is a member of the advisory team of the Naval Postgraduate School's Center for Asymmetric Warfare, serves as general counsel of the RIM Council of the Ponemon Institute, LLC, is a member of APCO Worldwide's International Advisory Council and previously served as co-chair of the Survey Committee of the American National Standards Institute's report on PHI, as well as on the privacy and the legal subcommittees of the PSAB of the Health and Human Services Agency, California Office of HIPAA Implementation.

His publications include *Information Security and Privacy: A Guide to Federal and State Law and Compliance* and *Information Security and Privacy: A Guide to International Law and Compliance*.

Tina Stow is a vice president in APCO Worldwide's Washington, D.C., corporate communication and issues management service group—a practice that helps Fortune 500, trade association and nonprofit clients develop and execute communication strategies that build their businesses, manage and mitigate risk, and engage their stakeholders.

Since joining APCO in 2010, Ms. Stow has provided strategic counsel and represented clients across multiple industries—guiding initiatives and campaigns encompassing corporate communication, public affairs, litigation communication, issues management and regulatory affairs, among other matters. Prior to joining APCO, Ms. Stow served as senior director of privacy and communications for technology and information company LexisNexis.

A member of the International Association of Privacy Professionals, Ms. Stow is a Certified Information Privacy Professional, a business line leader within APCO's issues management practice and a leader of APCO's D.C.-based privacy and information management offering, a part of APCO's technology practice.

The Lares Institute is a think tank that conducts independent research and releases policy proposals focused on technology, privacy and information governance, as well as issues impacting economic growth in the Southern California region. The Lares Institute draws on the experience of Andrew Serwin, who serves as CEO and executive director; Dr. Larry Ponemon, who serves as senior research advisor; and Congressman Ron Packard, who serves on the Institute's Advisory Board.

Founded in 1984, **APCO Worldwide** is an award-winning, independently owned global communication, stakeholder-engagement and business-strategy firm with offices in major cities throughout the Americas, Europe, the Middle East, Africa and Asia. APCO clients include corporations and governments; industry associations and nonprofit organizations; and six of the top 10 companies on the Fortune 500. The firm is a majority women-owned business.

EXECUTIVE SUMMARY

PRIVACY IS A CONCEPT THAT societies use to express concern over, and impose limits upon, the collection and use of information—in essence a societal safety valve on the collection and use of information. Privacy as a concept in the United States was strongly influenced by two leading scholars in the early twentieth century—Samuel D. Warren and Louis D. Brandeis, who popularized the "right to be let alone" in their law review article "The Right to Privacy." Both Warren and Brandeis recognized the influence technology had on privacy, as well as the importance of societal views regarding privacy, concepts that are also recognized now in the United States, as recent reports from the Federal Trade Commission demonstrate. Despite this recognition, at this time there is not a widely-accepted theoretical construct for privacy that looks at what individuals' expectations are and creates a workable solution in an economy driven by information. In short, technological advancement has made prior privacy models unworkable, and policy-makers and businesses alike recognize the failing of current privacy models to address these issues.

Societal concern over privacy is at an all-time high, and information-sharing will only accelerate over time as the inexorable advancement in technology permits an ever-increasing amount of information collection and processing, and this means that privacy concerns will only intensify as the technology of information sharing continues to advance. In light of the rapid changes in technology, it is all the more critical to have a unifying concept for privacy, such as the right to be let alone, because having an agreed-upon concept organizes and provides structure to societal norms, as well as laws, that help society define privacy. "Privacy 3.0—The Principle of Proportionality" is that principle. It looks at what individuals actually think about privacy, including their views of the sensitivity of certain forms of information, and sets proportional protections around information. This is all the more true if Privacy by Design (PbD) becomes a concept that more companies utilize. PbD helps companies design privacy into their products and services in a "proactive" and "user-centric" way, but PbD as a concept does not provide the data—a blueprint—to help companies understand what consumers are really concerned about.

This study represents the first step in creating that blueprint. It examines prior models of privacy, as well as the current thinking from the FTC regarding privacy, and argues that the model for privacy in the information-centric world we live in must be based upon an examination of data sensitivity (what individuals and societies think about privacy) and proportional protections that are based upon data sensitivity. The study also provides previously unreleased data regarding individuals' perceptions of privacy, as well as a detailed examination of what individuals think about the sensitivity of certain common forms of data.

In light of the rapid changes in technology, it is all the more critical to have a unifying concept for privacy, such as the right to be let alone, because having an agreed-upon concept organizes and provides structure to societal norms, as well as laws, that help society define privacy. "Privacy 3.0—The Principle of Proportionality" is that principle.

By accepting the Principle of Proportionality as the theoretical construct of privacy and using this information regarding sensitivity, society can begin to create a workable blueprint for privacy in a world driven by information. That blueprint will continue to evolve, as it will be important to do further research that examines what impact the context of information, including how the information is being used, impacts consumer perception. However, that evolution cannot begin without an examination of data sensitivity.

For more information about **The Lares Institute**, please contact **Andrew Serwin** at 858.735.6552 or andy@laresinstitute.com.

For more information about **APCO Worldwide's global privacy and information management offering**, please contact **Tina Stow** at 202.778.1026 or tstow@apcoworldwide.com.

INTRODUCTION

PRIVACY IS A CONCEPT THAT societies use to express concern over, and impose limits upon, the collection and use of information. It is a core issue to any society because it helps to define a number of important issues, such as how government can gather and use information (*e.g.,* restrictions on unlawful search and seizure); what information your employer can use to determine whether to employ you or not (*e.g.,* employee privacy rights under laws like the Fair Credit Reporting Act [FCRA]); what information private companies can gather about you to use for a variety of purposes; and issues such as reproductive rights, which have as their fundamental basis the right of privacy that prevents an invasion into some of the most intimate areas of our lives, as well as many other rights that we enjoy on a daily basis.

Societal concern over privacy is at an all-time high, in large part due to the fact that we live in an age defined by information-sharing, and the ability to rapidly collect, process and transmit information has transformed how we live, what products and services we buy, and even how governments function. Information-sharing will only accelerate over time as the inexorable advancement in technology permits an ever-increasing amount of information collection and processing, and this means that privacy concerns will only intensify as the technology of information sharing continues to advance. Technology, however, only tells us part of the picture regarding information sharing, because while technology is the vehicle we use to collect and process information, it does not define the ground rules for how information should be used. In short, as observed by Samuel D. Warren and Louis D. Brandeis in 1890, once again, "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person."[1]

The ground rules for societal issues such as privacy are instead set both informally as well as formally, independent of the technology that is used to collect and process information. Whether formal or informal, the goal of societal rules is to change the behavior of individuals to conform to societal expectations. When these expectations are informal, they are societal norms. Norms are informal rules, the violation of which have informal consequences, and norms help informally regulate social interactions through "shared expectations of behavior" that define what is appropriate and desirable in particular social interactions.[2] An example is your Facebook-addicted "friend" who repeatedly posts embarrassing pictures of you. While there is no spoken rule or formal consequences to this behavior, informal societal rules would predict that this person may not be a "friend" for long. In the business setting, we talk about "brand" damage to companies that use information in ways that customers do not like. Like the over-posting Facebook friend, informal societal norms would predict that the company also would find itself fresh out of "friends" that buy the company's products or services if individuals disapprove of the business practices.

When informal rules and sanctions are not sufficient to regulate an important societal issue, laws can be enacted to address the concern. As with societal norms, the goal of law is to regulate behavior, though it is done through formal requirements and consequences that mainly, but not always, track shared societal expectations. If you violate a law, rather than losing friends on Facebook, you might find yourself facing government sanction for violation of laws.

In the United States, privacy has always been a key concern, but it gained prominence as a stand-alone concept due to a key law review article written in 1890 by two preeminent legal scholars—Samuel D. Warren and Louis D. Brandeis. Concerned about advances in technology, instant pictures and journalists publishing facts without consent, which were disrupting societal norms, Warren and Brandeis wrote "The Right to Privacy," which sought to define that most personal protection of privacy in light of "[t]he intensity and complexity of life," "advancing civilization," and the invasions that "modern enterprise and invention" were creating.[3]

This very personal concern over "the moral standards of society as a whole"[4] led to the recognition of the "right to be let alone." The right to be let alone was, in the Warren and Brandeis model, implemented through the common law, due to the inherent flexibility of the common law to "grow to meet the demands of society" and to account for other societal factors such as political, social and economic changes to society.[5] The right to be let alone became the driving force behind privacy in the United States for many

years. Indeed, their article on privacy is indisputably the most cited law review article and recognized as the basis of many privacy laws that followed is publication. One noted scholar, Roscoe Round, concluded that it did "nothing less than add a chapter to our law."[6]

The right to be let alone is indisputably a significant intellectual contribution to privacy, but there are three other important points that the work of Warren and Brandeis also illustrate—technological advances cause reactive changes to societal norms and laws; subjective concerns are core to privacy; and it is important to have an overarching theory that helps to coalesce and drive societal norms and laws. These important issues are critical because we now find ourselves as a society facing the same issues that Warren and Brandeis did—how do we as a society define privacy in an era of rapidly advancing technology, and what should the theory of privacy be? There is significant concern over this issue, including by a number of government regulators, as is reflected by the FTC's most recent report on privacy, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*.[7] In that report, the FTC made a number of proposals, but there is no clear consensus regarding the future path of privacy.

However, the very technology that drives increased information-sharing and its attendant risks also provides current scholars a new path that was unavailable to Warren and Brandeis—detailed research regarding consumer perceptions of privacy. The purpose of this article is to help businesses and policy-makers recognize that privacy is a subjective societal issue that must be defined, in large part, by cutting-edge research regarding consumer perceptions of data sensitivity and the proportional protection of information.

This article will help to define the path forward for privacy by:

1. Examining the subjective and undefined nature of privacy currently
2. Creating a timeline that illustrates the prior path of privacy and the growing importance of information sensitivity and proportionality, including prior proportionality research
3. Illustrating the importance of the creation of a privacy "blueprint," including through PbD and consumer perception
4. Providing data regarding consumer perception of data sensitivity around 100 common data elements
5. Providing data to illustrate the importance of consumer perceptions regarding data sensitivity, as well as the impact of demographic issues
6. Proposing a path toward a future privacy framework

This article represents a first step forward to creating this framework, but future research will need to be done to complete the blueprint. This will include examining how the context, or use of information, impacts consumer perception, and examining the level of consumer knowledge regarding existing data sharing structures. However, this later research cannot truly be accomplished until data sensitivity is more fully examined, and this article offers the first concrete data regarding consumer perceptions and data sensitivity.

The right to be let alone is indisputably a significant intellectual contribution to privacy, but there are three other important points that the work of Warren and Brandeis also illustrate—technological advances cause reactive changes to societal norms and laws; subjective concerns are core to privacy; and it is important to have an overarching theory that helps to coalesce and drive societal norms and laws.

PRIVACY IS A SUBJECTIVE ISSUE THAT IS CURRENTLY UNDEFINED

WHILE SOCIETAL CONCERN OVER PRIVACY clearly drove Warren and Brandeis's thinking regarding the right to be let alone, there is not a uniform and clear focus on the subjective nature of privacy. This section will examine the issue and demonstrate that privacy is inherently a subjective societal issue and also show that little to no research has been done to attempt to define with specificity what individuals think about the sensitivity of information, though approaches to privacy focused on information sensitivity are beginning to come into focus.

PRIVACY IS A SUBJECTIVE ISSUE

Given the diverse views regarding privacy, it is important to have a common understanding to help frame the privacy debate. Privacy 3.0 raised the subjective nature of privacy when it noted that "Individual concern over privacy has existed for as long as humans have said or done things they do not wish others to know about."[8]

Put in different terms, as noted above, privacy is the name we give the ability (or right) to keep people from knowing certain things about you, or to use certain forms of information about you. Thus, there are really two elements to it—control of information (the ability to keep people from knowing certain things about you or using information in a way you do not agree with), based upon a subjective personal preference (the information we are concerned about here is information that a particular individual does not want others to know or use).

In most societies, the subjective personal preference is limited in certain ways by what society deems to be reasonable[9], but even accounting for reasonable limitations imposed by society, *what we are ultimately saying is that privacy is a very personal issue that is based upon individuals' subjective concern over the collection and use of information.*

Such an approach is not inconsistent with the approach of Warren and Brandeis, whose article was written in an era when detailed consumer research was not possible as it is today. While "The Right to Privacy" does not expressly label privacy subjective, it is clear that Warren and Brandeis recognized the role society played in defining privacy. When attempting to define this inherently personal protection, Warren and Brandeis recognized that societal rights such as privacy were impacted by political, social and economic changes and that law must grow to meet the demands of society.[10] Though Warren and Brandeis ultimately framed their discussion around the right to be let alone and did not explicitly advocate for an examination of individuals' view regarding the sensitivity of information, the information that Warren and Brandeis were concerned about was inherently sensitive. Moreover, their reliance upon common law and its ability to adapt to meet new societal concerns is consistent with an approach that recognizes subjectivity regarding the sensitivity of information, with concomitant proportional protections.

The subjective nature of information sensitivity is also reflected in the FTC Final Report. In its long-awaited final report on privacy, the Federal Trade Commission recently proposed a new privacy framework for businesses and policy-makers. The final report provides a significant amount of guidance on privacy, including a number of proposals that utilized data sensitivity and proportionality as a basis for examining privacy in this information-centric economy.[11]

> The Commission is cognizant, however, that whether a particular piece of data is sensitive may lie in the "eye of the beholder" and may depend upon a number of subjective considerations.[12]

The final report, released in March 2012, represents the FTC's final thinking on a privacy framework it first proposed in 2010. This framework links a number of privacy issues to data sensitivity or proportionality, including:

- The scope of the application of the FTC's proposed framework
- Consumer access to information, including related to certain legislative reforms
- The context of certain choices that are offered to consumers
- The reasonableness of security
- The accuracy of data
- Choices consumers have regarding the collection of information for first-party marketing
- Specific issues related to data brokers

The final report also illustrates one of the current limitations on using data sensitivity as the construct of privacy—there is not sufficient data regarding consumer views about data to make completely informed decisions.

THERE IS NO CONSENSUS ON HOW TO DEFINE SENSITIVITY

Even in the most recent FTC report, there was not consensus regarding what information is considered sensitive. While a number of commenters provided their views regarding data sensitivity, and there was "general consensus" among the commenters that heightened consent was required for "sensitive" information, such as "information about children, financial and health information, Social Security numbers, and precise, individualized geolocation data," there was not consensus among the commenters regarding whether information "related to race, religious beliefs, ethnicity, or sexual orientation, as well as biometric and genetic data" was sensitive[13]. In one more extreme example, one commenter believed that information related to "consumers' online communications or reading and viewing habits" was sensitive. Interestingly, the FTC stated that some commenters noted the "inherent subjectivity" of this inquiry.[14]

While the FTC relied upon its own experience, as well as the suggestions of commentators, there was neither a study of consumer perceptions regarding data sensitivity, nor any actual data in the FTC's report, to support these statements, other than the comments themselves.

While the FTC relied upon its own experience, as well as the suggestions of commentators, there was neither a study of consumer perceptions regarding data sensitivity, nor any actual data in the FTC's report, to support these statements, other than the comments themselves. This presents a challenge for regulators such as the FTC, as well as businesses that must attempt to implement privacy-protective programs. Indeed, when one examines consumers' perceptions regarding these data elements referenced above, some are considered by consumers to be sensitive, and others are not.

One could examine what privacy laws protect, which at times is a proxy for consumer concern, or examine the positions of advocacy groups, which might be reflective of consumer concerns as well, to try to ascertain what individuals are concerned about. One could even examine the business models of certain companies regarding information, and see if consumers make choices based upon the practices, but beyond those three things, there is not a lot of guidance about individuals' subjective concern over what information they do not want others to know. This lack of information is particularly problematic given some of the proposed solutions to privacy concerns, particularly those in the Web 2.0 world.

In conclusion, there are two key points to understanding what privacy really is: (1) privacy is a personal issue based upon subjective beliefs; and (2) there is not clear data or research regarding consumers' subjective beliefs regarding the sensitivity of information.

TIMELINE OF PRIVACY MODELS, KEY FTC EVENTS AND PROPORTIONALITY

IN ORDER TO UNDERSTAND THE PATH forward for privacy, it is critical to understand where we have been. Understanding the progression of privacy in society will help us understand what has been tried in the past, what the FTC has used as its basis for enforcement, and why proportional protections based upon sensitivity offer a path forward that uniquely fits today's societal concerns.

1890: Warren & Brandeis publish "The Right to Privacy," one of the most widely cited law review articles.

1960: Prosser publishes "Privacy," which becomes the basis of the Restatement Torts (Second), and is also widely cited.

1970: The Fair Credit Reporting Act (FCRA) is passed, and the FTC gains direct privacy jurisdiction.

2000: The FTC utilizes "notice and choice" as its privacy model.[15]

Early 2000s: The FTC utilizes harm-based issues as the privacy model.[16]

2008: "Privacy 3.0—The Principle of Proportionality," is published, and has since been cited by numerous law reviews, including the *Berkeley Technology Law Journal*, the *Harvard Journal of Law & Technology*, and the *University of Iowa Law Review*.

2010: The FTC issues its *Preliminary Report Protecting Consumer Privacy in an Era of Rapid Change* and data sensitivity and proportionality are discussed in some detail, and the FTC's privacy framework is first proposed.

2011: "The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices," is published, as is "The Demographics of Privacy—A Blueprint for Understanding Consumer Perceptions and Behavior," which has been cited by the American National Standards Institute (ANSI).

2012: The FTC's final report, *Protecting Consumer Privacy in an Era of Rapid Change*, is published and explicitly relies upon proportionality and sensitivity in a number of ways, and the privacy framework is modified in certain ways and is placed in final form.

THE RIGHT TO PRIVACY—PRIVACY 1.0: ADOPTED 1890

The privacy construct created by Warren and Brandeis is one that is familiar to many people. It is one that has been summarized in many articles, and one that has been characterized as Privacy 1.0. Privacy 1.0, characterized by the right to be let alone, was driven by the technological concern of the time—the instant camera. In this article, Warren and Brandeis rejected the harm-based models that would become the norm following Privacy 2.0, and by adopting the right to be let alone effectively adopted a notice- and choice-based model of privacy, as one cannot truly exercise the right to be let alone unless there is notice—an understanding of the potential privacy invasion, and choice—the freedom to determine when and where one's information is disclosed or used.[17] This model did not expressly rely upon data sensitivity as the underlying theoretical construct of privacy, though its reliance upon the flexibility of common law to shape the right at least indirectly incorporates subjective concerns of society into the right to be let alone.

PROSSER'S PRIVACY—PRIVACY 2.0: ADOPTED 1960

Prosser's formulation of privacy focused on a common-law harms-based approach that ultimately was tied to four tort causes of action that became part of the Restatement of Torts. This model did not directly focus on sensitivity, and instead focused on harm.[18]

NOTICE AND CHOICE PREVAILS AT THE FTC: 2000

The FTC, after the enactment of the FCRA, attempted to get businesses to comply with certain privacy principles—the Fair Information Practice Principles (FIPPs)—and even suggested legislation based upon the FIPPs, which included notice and choice. Moreover, the FTC extensively used its "Deception" jurisdiction, which is inherently a notice-and-choice type of analysis, because deception focuses on what the consumer was told and whether the consumer could, and in some cases did, make a choice based upon the notice he or she was provided.[19] The important thing to note is that proportionality and sensitivity were not the focus of this model.

HARM-BASED-MODELS PREVAIL AT THE FTC: EARLY 2000s

Notice and choice did not ultimately prevail at the FTC as the main enforcement model, and the FTC began to focus more on consumer injury, particularly in the data breach arena. Ultimately, the FTC also began using its unfairness authority, which is an analysis focused on consumer harm. Like notice-and-choice models, harm-based models do not sharply focus on data sensitivity or proportionality.[20]

"PRIVACY 3.0—THE PRINCIPLE OF PROPORTIONALITY": 2008

Privacy 3.0 represented a departure from the right to be let alone, as well as harm-based models. Based upon the Principle of Proportionality, Privacy 3.0 was designed to provide appropriate, but not over-inclusive or under-inclusive protection, particularly in the rapidly changing Web 2.0 world where information sharing was the basis of a number of now-ubiquitous services that consumers desire. Privacy 3.0 also recognized that society would benefit from information-sharing, though there should be restrictions, or use limitations, on the sharing.[21]

The advantage of this model is that it places higher restrictions and access barriers on truly sensitive information that either has limited or no use to third parties and has great capacity to damage individuals and society, while simultaneously permitting the necessary and appropriate access to those having a legitimate need to know certain information, particularly when that information is less sensitive. Proportionality also has the advantage of minimizing the societal impact of privacy issues because enforcement and compliance will be focused on the most appropriate levels of sensitive information.

In other words, the protections, use and other limitations related to information should be proportional to the sensitivity of data. Among the issues that Privacy 3.0 noted to be derived from sensitivity were:

- whether information can be gathered without notice or consent
- whether consent must be opt-in or opt-out
- the effect of consent
- the types of processing that can be done
- whether information can be gathered under false pretenses
- whether there are time restrictions upon the retention of the data
- data security requirements
- data destruction requirements
- what steps are required, or permitted, to mitigate any mishandling of information
- penalties for misuse of the information, including the imposition of statutory penalties in certain cases

FTC PRELIMINARY REPORT—PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: 2010

The FTC began creating its most recent privacy framework in 2010 via the preliminary report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*.[22] This report identified a number of key issues and concerns in the Web 2.0 world. The FTC correctly noted that consumer information has become increasingly critical in the digital economy and that companies are continuing to create innovative ways to provide new and better products and services. In the FTC's view, while some companies were appropriately protecting consumers, others were not. There was also concern expressed by stakeholders to the FTC regarding improving transparency, simplifying choice for consumers, and making sure that businesses adopt proactive privacy protection measures as new systems that collect and process information are created and implemented.

The FTC noted concerns that were expressed regarding over-regulation and that certain commenters had "urged regulators to be cautious about restricting the exchange and use of consumer data in order to preserve the substantial consumer benefits made possible through the flow of information," because the exchange of data "not only helps to fund a variety of personalized content and services, but also allows businesses to innovate and develop new products and services that offer consumers convenience and cost savings."[23]

The proposed framework focused on several elements including: applying the framework to entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device; promoting

consumer privacy throughout organizations and at every stage of the development of their products and services; simplifying consumer choice; and increasing transparency.

THE FEDERAL TRADE COMMISSION AND PRIVACY: DEFINING ENFORCEMENT AND ENCOURAGING THE ADOPTION OF BEST PRACTICES: 2011

The Federal Trade Commission and Privacy article argued that the FTC should adopt Privacy 3.0 as a model to encourage the adoption of best practices. By using data sensitivity to help define a number of issues, including the safeguards required to be implemented for personal information, and that the uses and restrictions regarding information be contextually connected to the sensitivity of that information, the FTC could regulate the use of information without stifling innovation or preventing consumers from realizing the benefits of the use of information in our economy. Moreover, the use of Privacy 3.0's proportional protections based upon data sensitivity would permit "the safeguards required to be implemented for personal information contextually connected to the sensitivity of that information using a proportional methodology."[24] This article also noted that the use of sensitivity to drive proportional protections would permit the approach to be flexible as technology advanced, and also permit the FTC to approach the issue with a method that did not result in over- or under-regulation.

THE FTC'S FINAL REPORT—PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: 2012

The FTC's final report considers a number of different issues, as well as the significant amount of comments the FTC received, and proposes a framework for companies and policy-makers. A number of things are notable, including the numerous references to sensitivity and proportionality, as well as the general lack of agreement on what data is sensitive, including the explicit recognition that this issue at times can be "in the eye of the beholder."[25]

One clear indication of the importance of sensitivity to the FTC's final framework is that the applicability of the framework is tied to sensitivity. The framework in the preliminary report purported to apply to entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. The final report changed the scope of the application of the framework so that it did not apply to entities that collect *non-sensitive data* from fewer than 5,000 consumers per year and if they do not share the data with third parties.[26] The FTC also noted that companies could attempt to implement the final framework in a way that "… is proportional to the nature, sensitivity, and amount of data collected, as well as to the size of the business at issue."[27]

The FTC also explicitly stated that it agreed with the commentators who had suggested that affirmative express consent was appropriate when a company uses *sensitive* data for marketing, whether first- or third-party marketing.[28] It also recognized the role of sensitivity in implementing consumer choice issues, including those related to notice.[29]

In summary, examples of the issues that the FTC tied to sensitivity were:

- Consumer access to information, including related to certain legislative reforms[30]
- The context of what choices are offered to consumers[31]
- The reasonableness of security[32]
- The accuracy of data[33]
- Choices consumers have regarding the collection of information for first-party marketing[34]
- Specific issues related to data brokers[35]

PRIOR MODELS HAVEN'T SOLVED TODAY'S ISSUES, AND DATA SENSITIVITY AND PROPORTIONALITY ARE GAINING FAVOR

Privacy 1.0 and 2.0 each played a role in helping to drive behavior regarding privacy, including serving as the basis for the adoption of a number of laws and regulations. However, it is recognized that the prior models, based upon notice and choice and harm, have not kept pace with today's societal concerns. Though there is no consensus regarding the next evolution of privacy, regulators such as the FTC have recognized the importance of PbD, a doctrine that encourages the proactive design of privacy, and also started focusing more upon data sensitivity and proportional protections.

The path for proportional protection of privacy based upon data sensitivity is not a path that is unexplored. "Privacy 3.0—The Principle of Proportionality," and works following that article, offer a path forward if proportionality and sensitivity are recognized as being central to the privacy debate.

PRIVACY, SUBJECTIVITY AND PROPORTIONALITY

BASED UPON THE FAILURE OF other models and the growing recognition of proportional protections based upon information sensitivity, strong consideration must be given to the adoption of Privacy 3.0 to help guide the future of privacy. In order to operationalize this concept, PbD can be utilized, in conjunction with consumer research, to create a blueprint for privacy.

PRIVACY BY DESIGN (PbD)

PbD is a doctrine that has gotten a lot of attention as a potential solution to privacy concerns, including in the FTC's final report. PbD focuses on helping companies proactively design privacy into products and services:

> The privacy by design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred—it aims to prevent them from occurring. In short, privacy by design comes before-the-fact, not after.[36]

Moreover, the seventh principle of PbD focuses on respecting individuals' privacy by keeping it "user-centric."[37] Accepting PbD as a probable solution to privacy concerns, the next question to ask is obvious—*how do you proactively design privacy in a way that accounts for individuals' subjective concerns about information they do not want other people to know?* The answer is actually simple—determine what individuals' subjective concerns are about information before you attempt to design privacy.

While PbD has helped advance the debate, there is not an existing "blueprint" to understand individuals' subjective concerns about information. Said differently, the challenge is that companies are not really designing privacy, at least in a way that accounts for consumers' expectations in a user-centric way. To put this in real terms, it is like hiring a contractor to build a house, without any input from the homeowner. While the contractor might get some things right, he will also get a lot of things wrong, and at best the homeowner will likely be either very unhappy or at least marginally unhappy—a situation that sounds remarkably reminiscent to the some of the complaints we hear today about privacy.

While PbD has helped advance the debate, there is not an existing "blueprint" to understand individuals' subjective concerns about information…the challenge is that companies are not really designing privacy, at least in a way that accounts for consumers' expectations.

The solution to this is simple in concept but will take time and effort to create—and that is to create a true blueprint for consumer expectations regarding privacy. This process started with the release of the Lares Institute's study "The Demographics of Privacy—A Blueprint for Understanding Consumer Perceptions and Behavior," which provided unique insight into consumers' views about privacy, their own privacy protective behavior, as well as their privacy sensitivity regarding certain classes of information. What follows is new information regarding consumer perception of the sensitivity of information, placed in quartiles, as well as a summary of the prior research from The Demographics of Privacy study.

This information serves as the beginning of a blueprint for businesses to better understand what consumers are concerned about, as well as how, at some level, to predict consumer concerns based upon self-professed privacy sensitivity, in addition to demographic factors.

DATA ELEMENTS AND DATA SENSITIVITY RANKINGS

THE DATA THAT FOLLOWS will help frame and inform the debate regarding what consumers' subjective beliefs regarding privacy and sensitivity are. While the demographic issues have been discussed in prior studies, the Lares Institute has not previously released the data elements with rankings. The Lares Institute asked individuals to rank the sensitivity of data elements on a 1-10 scale and then took those rankings and created a mean ranking for each data element. The data elements were then ranked in order from most sensitive to least sensitive by mean, and the following tables were created.

QUARTILE 1

This quartile includes a number of data elements you would expect, such as Social Security numbers, information regarding respondents' children and employment evaluations, which confirms some of the FTC's beliefs about consumer perception, but it also includes some information you would not perhaps expect, such as information regarding home security systems, and it does not include information that the FTC and commentators expected, such as geolocation, sexual orientation or religious background.[38]

1. Social Security number
2. Password or other personal identification number required to access an account or services
3. Credit card or other account number, including information associated with a credit card
4. Financial information, including income tax filings, and financial statements
5. Any ID or number assigned to an individual, including account numbers, user IDs or passwords
6. Payment card information (debit or credit card)
7. Account balances
8. Automated or electronic signatures
9. Information from the computer chip, magnetic strip of a credit or other payment card
10. Alien registration number, government passport number, employer identification number, taxpayer identification number, Medicaid account number, food stamp account number, medical identification number or health insurance identification number
11. Information regarding credit standing or worthiness, assets, or liabilities including a person's credit capacity, character, general reputation, personal characteristics or mode of living
12. Answers to security questions (for dual authentication purposes)
13. Information regarding a home security system
14. Biometric information or numerical representation of biometric data, including finger/voice prints, handwriting, etc.
15. Health plan beneficiary numbers
16. Information regarding income or other related information
17. Employee account information
18. Information regarding health insurance, including the existence of insurance or claims history
19. The content of electronic communication such as texts or emails
20. Employee ID
21. Employment evaluations, including information regarding disciplinary actions
22. Physician/laboratory test orders
23. Health insurance application information
24. Information regarding past, present or future health or conditions, including information regarding medical treatment
25. Information collected from the respondent's children

QUARTILE 2

Quartile 2 includes certain insurance and financial information, location-based information and certain forms of health information.

26. Information regarding insurance or insurance claim history
27. Serial numbers for any mobile device (cell phone or PDA)
28. Background check information
29. Any ID assigned to a respondent by a non-governmental agency
30. A persistent identifier, such as a customer number, that is combined with other identifiable information about the respondent
31. The identities of people respondents emailed or called
32. Voided checks
33. Information regarding prescription drugs taken by respondents
34. Prescription history
35. Location-based information
36. IP address
37. Cell or mobile device number, including unique device identifier (UDID) for a mobile device
38. Information regarding specific diseases a respondent might have
39. Personally identifiable dates, such as date of birth
40. Payment history for any services or products
41. Information regarding a government ID other than a driver's license
42. Government clearance information
43. Age or gender of children
44. Overdraft history
45. Information regarding non-financial accounts, including any house or similar accounts
46. Diagnostic images, such as x-rays, MRIs, or CAT scans
47. Purchase history at a drug store
48. Information regarding an application for homeowner's insurance
49. Any information on a phone bill
50. Information regarding employment

QUARTILE 3

This quartile includes information from medical devices, information regarding individual's residences, family health history, arrest records, drug testing information and home address, as well as photographs.

51. Information from medical devices
52. Vehicle identifiers and serial numbers, including license plates
53. Information regarding a respondent's residence other than address
54. Family health history
55. Information regarding participation in clinical trials
56. Arrest records
57. Mother's maiden name
58. Information regarding drug use or addictions
59. Drug testing information
60. Home address
61. Purchase history regarding online purchases
62. Information regarding searches on the Internet
63. Genetic information

64. Audio recordings of a respondent
65. Student identification
66. Telephone number
67. Photographs or videos of a respondent
68. A history of websites a respondent visited
69. Information regarding where a respondent has traveled, including airline records
70. Information regarding use of social networking services
71. Student records
72. Email address
73. The number of any professional, occupational, recreational or governmental license, certificate, permit or membership a respondent has
74. Information regarding a government-sanctioned professional license or other professional certification number
75. Current or former name

QUARTILE 4

There are certain surprises, including that certain social media information ranked this low, as well as certain "special" categories of information. The quartile is mostly categorized by a number of types of consumer purchase histories.

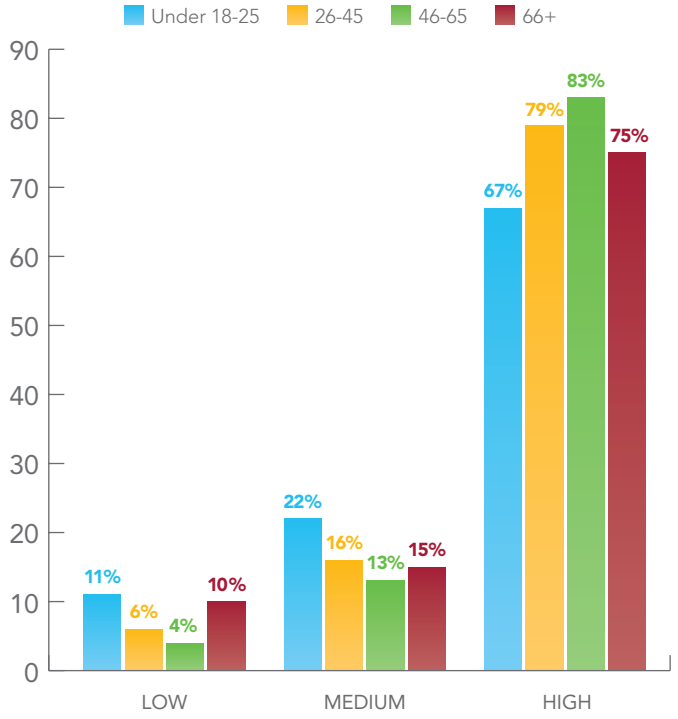
76. Information regarding criminal convictions
77. Instant message identifier
78. Information pertaining to service in the Armed Forces
79. Information regarding professional or employment history
80. Fax number
81. Information that reveals what hotels a respondent has stayed at
82. Place of birth
83. Information regarding sexual orientation
84. Purchase history of products or services
85. Information regarding use of apps, games, or other similar information
86. Grades from college
87. Information that reveals utility usage
88. Purchase history regarding purchases of books
89. Diet or exercise-related information
90. Information regarding your ethnicity, nationality or citizenship
91. Information regarding marital status
92. Occupation
93. Purchase history regarding a respondent's viewing of movies
94. Information regarding philosophical beliefs
95. Information regarding political beliefs
96. Educational history
97. What a respondent "likes" on Facebook
98. Information regarding religious beliefs
99. Information regarding games played online
100. Television viewing information

Further research will help expand and further define this list, but this list presents the next step in the blueprint of privacy.

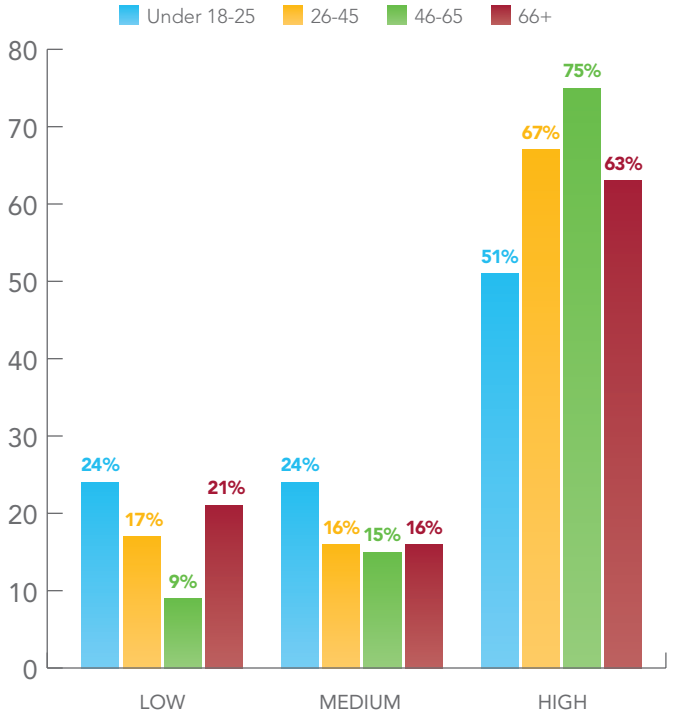
UNDERSTANDING PRIVACY SENSITIVITY

These graphs represent some of the information that was in *The Demographics of Privacy*, and they illustrate the impact of individual's self-reported privacy sensitivity and demographic factors. This first graph demonstrates that age impacts respondents' self-reported privacy sensitivity generally.

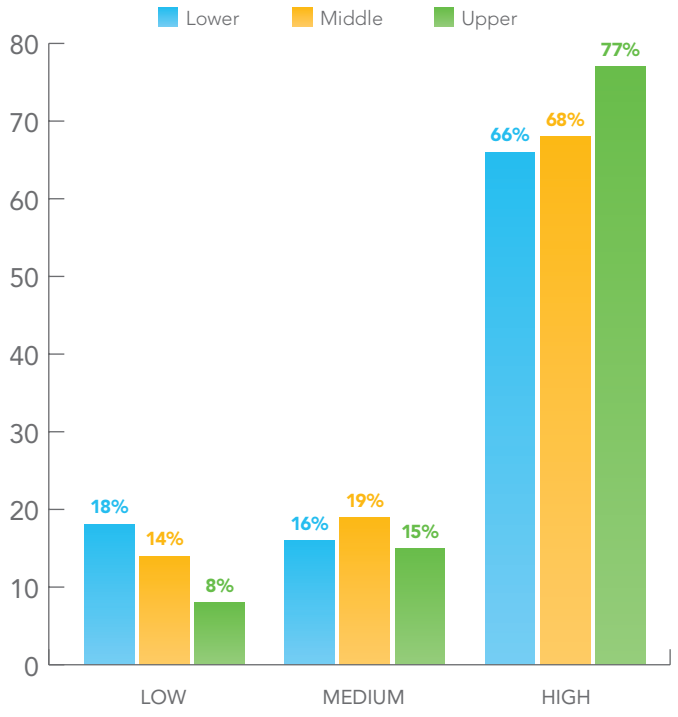
PRIVACY SENSITIVITY BY AGE



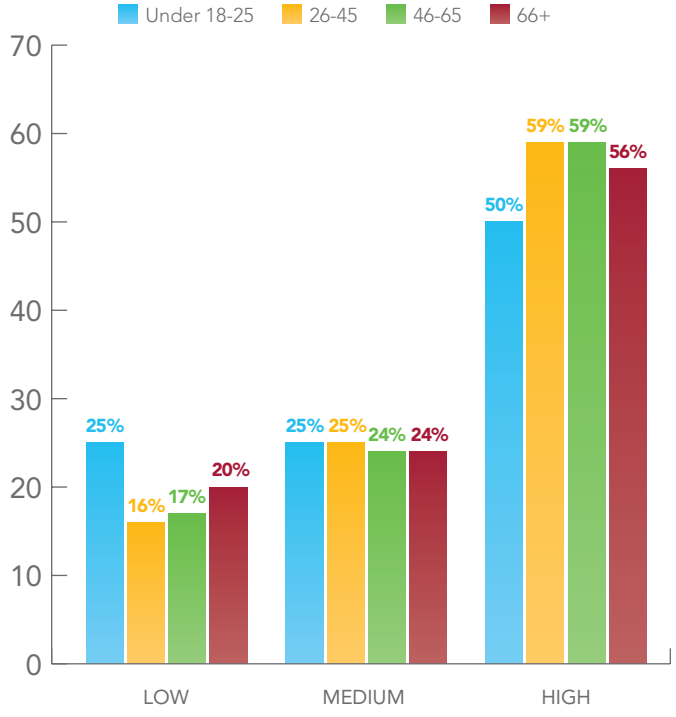
HEALTH INFORMATION SENSITIVITY BY AGE



HEALTH PRIVACY SENSITIVITY BY INCOME

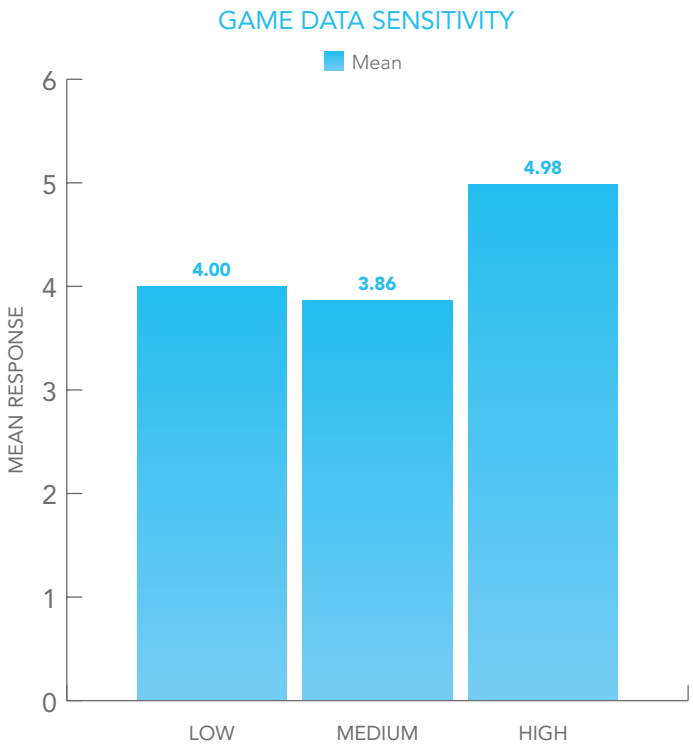


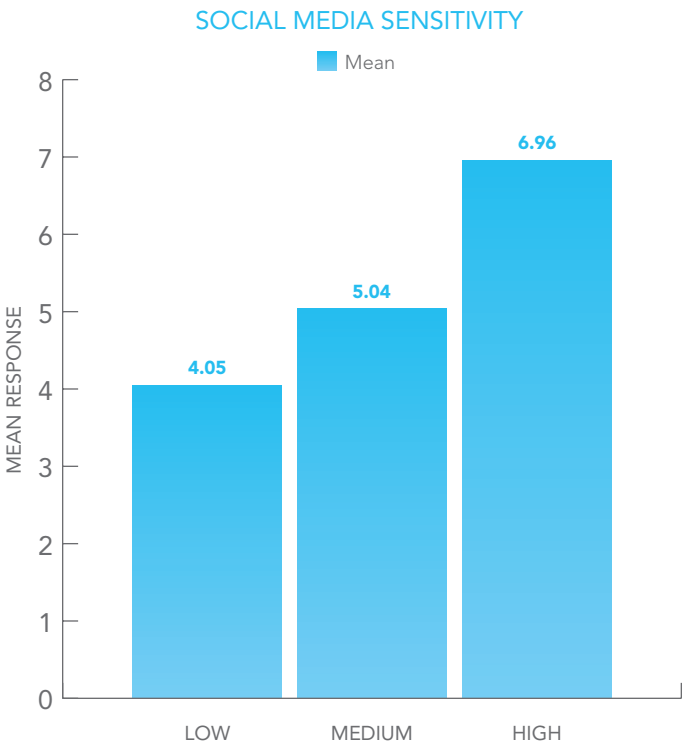
SOCIAL MEDIA PRIVACY SENSITIVITY BY AGE

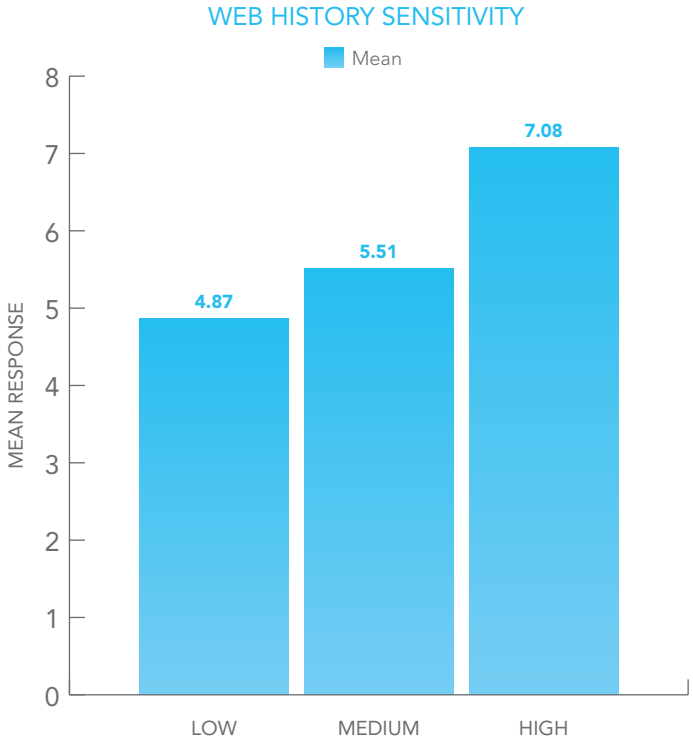


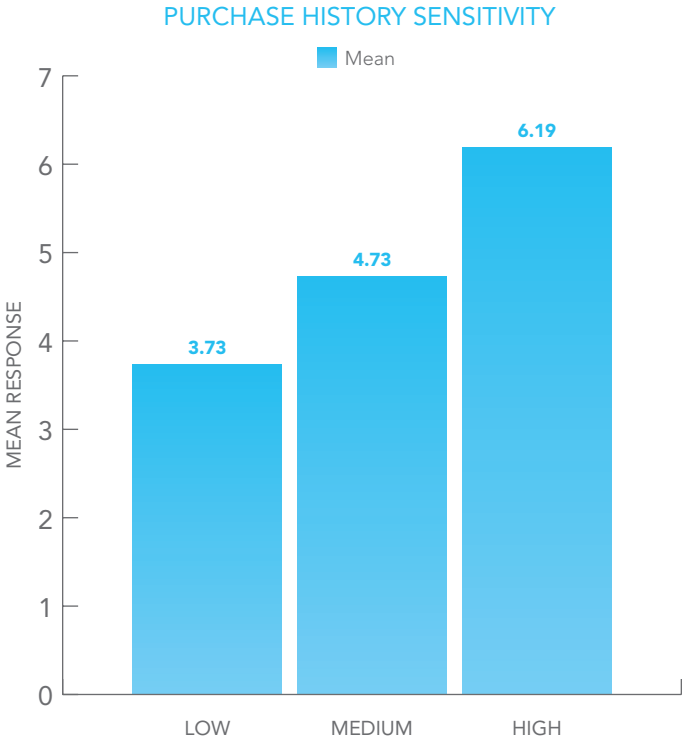
SELF-IDENTIFIED SENSITIVITY AND DATA-ELEMENT SENSITIVITY

One of the conclusions of the demographic study is that individuals' self-reported privacy sensitivity is predictive of how sensitive they are regarding certain data elements.

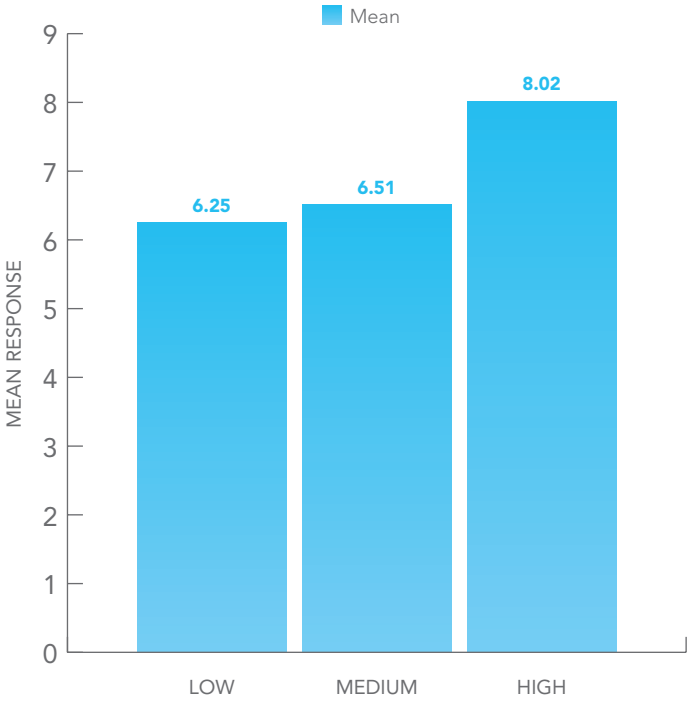




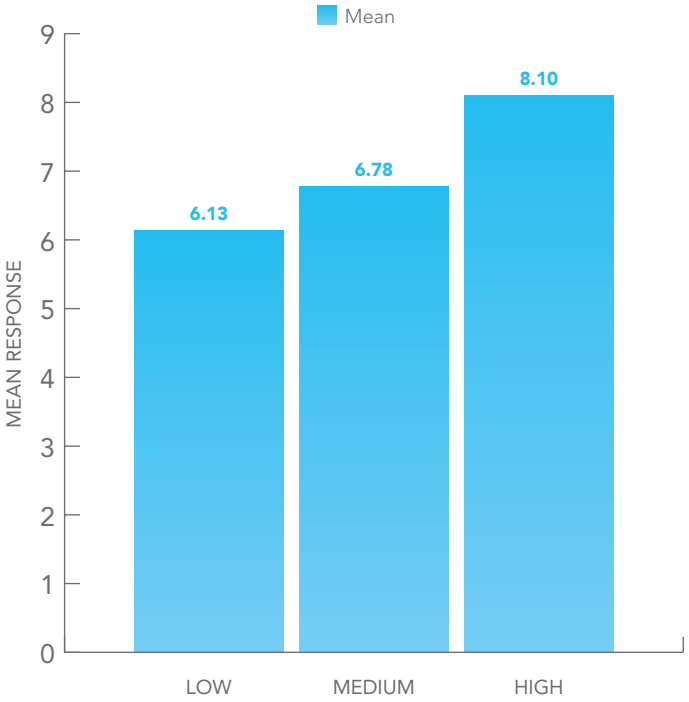




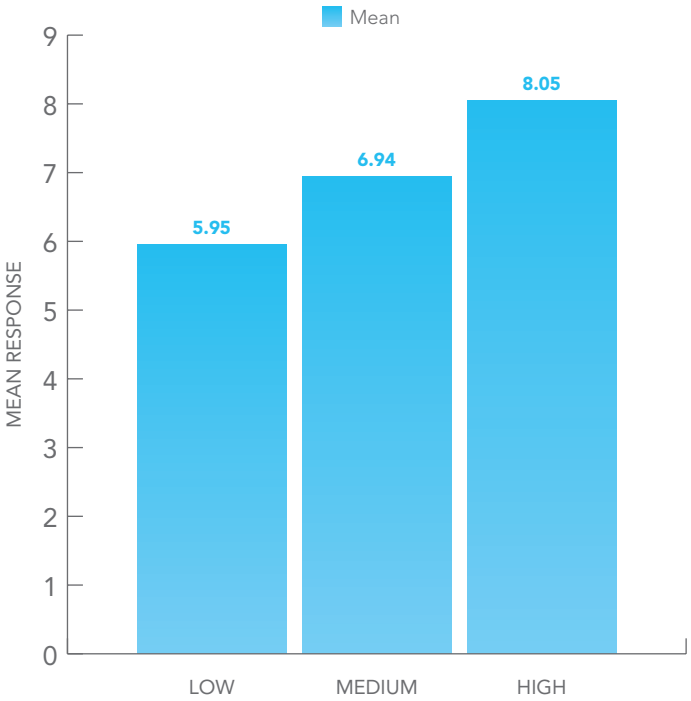
UNIFORM DEVICE IDENTIFIER (UDID) SENSITIVITY



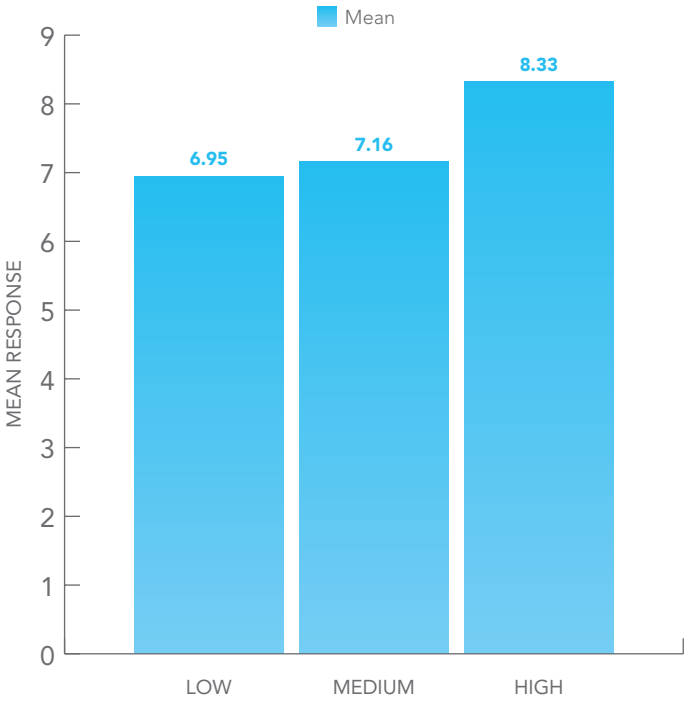
IP ADDRESS SENSITIVITY



ID OF CALLS AND EMAILS SENSITIVITY



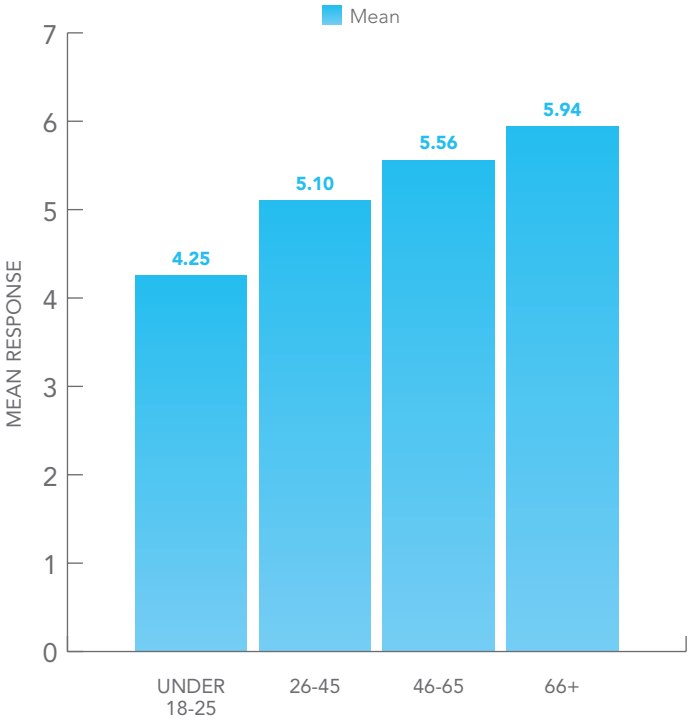
CONTENT OF COMMUNICATIONS SENSITIVITY



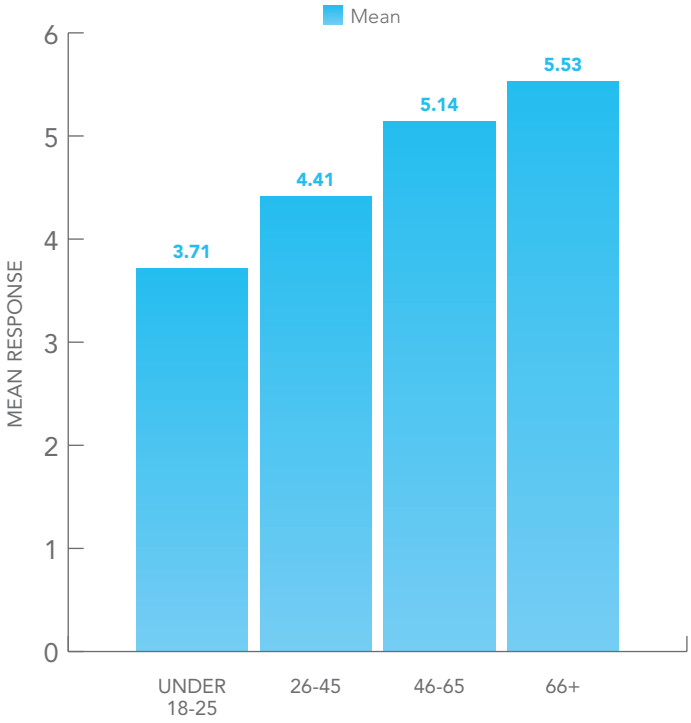
DEMOGRAPHICS AND DATA-ELEMENT SENSITIVITY

Demographic issues also impact individuals' perception of the sensitivity of certain data elements, and these graphs illustrate the impact of demographic factors.

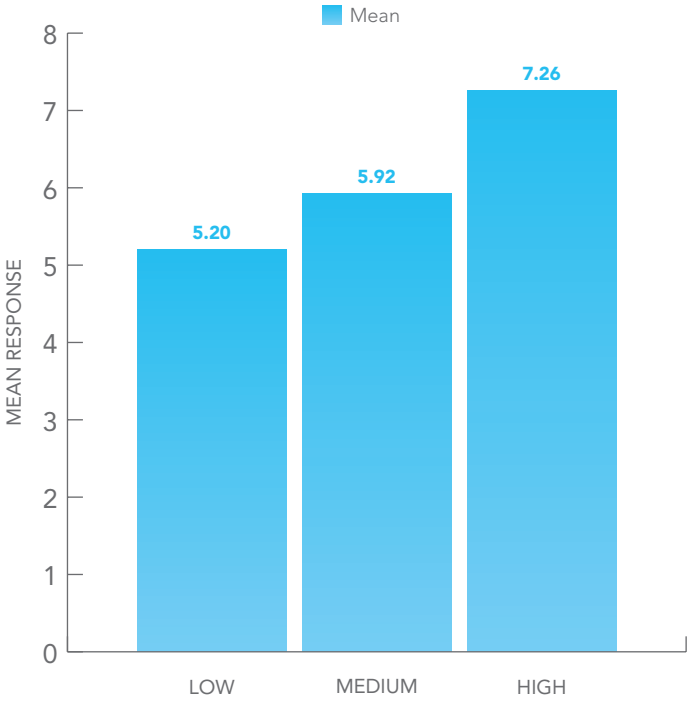
PURCHASE HISTORY AND AGE



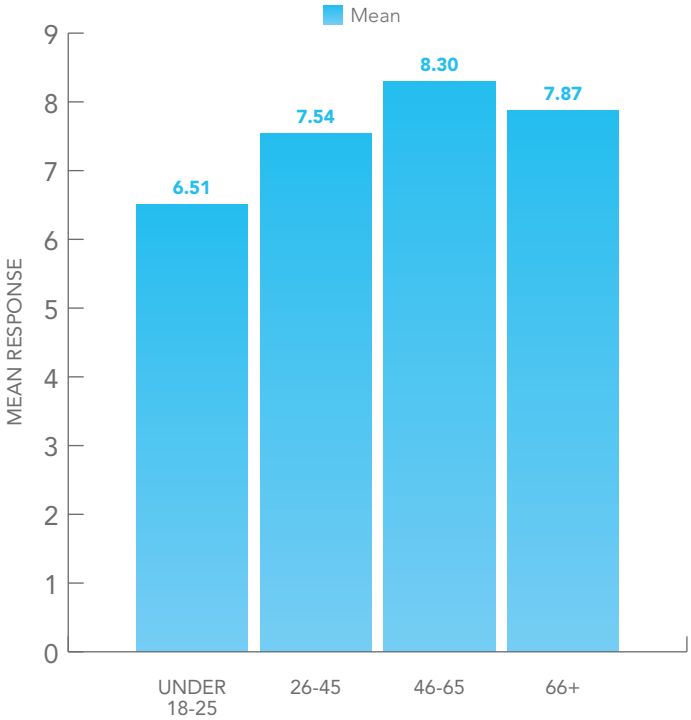
AGE AND LIKES



SENSITIVITY AND SEARCH INFORMATION



PERSISTENT IDENTIFIER AND AGE



CONCLUSION

PRIVACY IS THE SAFETY VALVE society imposes on the use and sharing of information. It is inherently influenced by technological advances, as well as societal views regarding information. We live at a time that is marked by rapid advances in technology related to information, which has caused prior privacy models to fail, because they do not work in the Web 2.0 world due to the rapid and pervasive nature of information collection and processing. This failing is critical because, as the influence of the right to be let alone demonstrates, the societal theory of privacy helps to define and organize societal norms and laws regarding information protection and helps societies come up with solutions that are clear and appropriate.

Privacy 3.0—The Principle of Proportionality, which is based upon individuals' views regarding data sensitivity, is the theory that should drive today's privacy debate. It examines what individuals think about privacy and helps to guide proportional protections that are reasonable and appropriate. This is all the more true if PbD becomes a concept that more companies utilize. PbD helps companies design privacy into their products and services in a "proactive" and "user-centric" way, but PbD as a concept does not provide the data—a blueprint—to help companies understand what consumers are concerned about. This paper represents the first step in completing the privacy blueprint, through the research regarding consumer perceptions of data sensitivity.

Now that this research has been released, it is appropriate to ask about the next steps to create a workable framework for business and policy-makers. First, while the recognition of the role of sensitivity and proportionality in documents such as the FTC's final report are important to demonstrate where policy is heading, Privacy 3.0 should be expressly adopted as the overarching construct for privacy, because this will help shape the debate and ultimately assist policy-makers and businesses considering the implications of proportionality and sensitivity. Second, the data regarding consumer perception and data sensitivity should also be incorporated into the privacy debate as the beginning of the privacy blueprint. It is the first real data policy-makers and businesses have to help inform the framework, including PbD. Third, further research that examines additional data elements, as well as how the context, or use of information, impacts consumer perception, needs to be completed, as does research that examines the level of consumer knowledge regarding existing data sharing structures. Fourth, businesses should consider the importance of this research as they continue to build models that seek to build consumer trust and enhance consumer experience. Fifth, since this research is based solely on individuals in the United States, international research needs to be done to see how different societies value and assess privacy.

A DESCRIPTION OF THE STUDY

THE STUDY IS BASED UPON several surveys that asked consumers to: rank their sensitivity regarding certain forms of information, as well as privacy generally; self-report on their own privacy protective behavior; self-report on their review of certain policies and agreements; rate 100 data elements on a 1-10 scale of how sensitive certain forms of information were; and provide certain forms of demographic information.

Results from this survey are based upon an Internet-based survey instrument that sent surveys to a representative sample of individuals, which resulted in a sufficiently large number of responses. These responses were part of three separate surveys which were sent to 954, 474 and 482 individuals in the United States; 818, 420 and 399 responses were respectively received, for a response rate of 85.7%, 88.6% and 83.6%. The margin of error of this survey is 5% at a 95% confidence level. The demographics of the survey sample generally track the U.S. Census, and are available upon request from the Lares Institute.

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings, such as non-response bias, as it is possible with any survey that individuals who did not participate would respond differently than those who did. Moreover, question wording, other survey concerns, and sampling error can result in error or bias in the findings of surveys. Finally, survey research is based upon the quality and integrity of confidential responses that the Lares Institute received from survey participants.

ENDNOTES

1 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193 (1890).

2 Oxford Dictionary of Sociology (2009).

3 Warren & Brandeis, *The Right to Privacy,* supra, note 1.

4 Warren & Brandeis, *The Right to Privacy,* supra, note 1.

5 Warren & Brandeis, *The Right to Privacy,* supra, note 1.

6 Daniel J. Solove, Marc Rotenberg, and Paul M. Schwartz, *Privacy, Information, and Technology* (Aspen Publishers, 2006).

7 Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers, FTC Report (March 2012).

8 Andrew B. Serwin, "Privacy 3.0—The Principle of Proportionality," 42 U. Mich. J.L. Reform 869 (2009), pg. 870.

9 When courts, at least U.S. courts, try to define the limits of fundamental privacy-related rights we do have in the United States—the Fourth Amendment right against unlawful search and seizure—the touchstone of the analysis is whether the individual (subjectively) has an expectation of privacy that society finds to be reasonable (an objective standard). Using the U.K. as an example, the extensive CCTV networks demonstrate that their society has decided that having CCTV throughout the country is important enough that anyone's subjective privacy concern is overridden if they choose to be in public, which isn't really a meaningful choice for an individual.

10 Warren & Brandeis, *The Right to Privacy,* supra, note 1.

11 The final report modified the Preliminary Report that was previously issued by the FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers. FTC Preliminary Report (2010).

12 Protecting Consumer Privacy in an Era of Rapid Change, supra note 8, pg. 60.

13 Protecting Consumer Privacy in an Era of Rapid Change, supra note 8, pgs. 58-59.

14 Protecting Consumer Privacy in an Era of Rapid Change, supra note 8, pgs. 58-59.

15 Andrew B. Serwin, The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices, 48 San Diego L. Rev. 809, 815-16 (2011).

16 Id.

17 See Serwin, supra, note 16, pages 817-18, internal footnotes omitted.

18 See Serwin, supra, note 16, pages 882-84, "In 1960, Dean Prosser examined a number of the cases that flowed from the Warren and Brandeis theory and categorized them into one of four categories, which ultimately served as the basis for the Restatement's four categories of privacy torts: intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a person in false light. … While the Prosser/Restatement model provides some additional framework to understand privacy concepts, it still relies on common law, and is still based in tort theory. Inherently, this limits its usefulness in addressing the privacy issues of today."

19 See Serwin, supra, note 16, pages 815-16, "For the FTC, the notice-and-choice model began in 2000, with the FTC recommending that Congress require businesses to comply with the fair information practice principles, which include notice-and-choice. Congress did not pass this legislation, so the FTC focused initially on raising public awareness, encouraging self-regulation, and also bringing cases under section 5 based upon its deception authority. Deception, as noted below, focuses on what "material" information the consumer was or was not told, particularly where the deception impacts a consumer's choice regarding goods or services. Moreover, although injury is a factor that is considered in deception cases, the analysis of injury is part of an examination of whether the allegedly misleading information was material, and actual injury is not required. Instead, the FTC must simply show that consumers are "likely to suffer injury from a material misrepresentation."

20 See Serwin, supra, page 816, "The second enforcement model, the harm-based approach, represented a departure from the notice-and-choice model. Although

the FTC continued to use deception in its cases, later cases focused more on actual consumer injury—typically resulting from an alleged breach—and the FTC began instead to rely more on its unfairness authority. As discussed below, the FTC's unfairness authority does not focus on what was told to the consumer but rather whether the consumer suffered "substantial" injury."

[21] Serwin, supra, note 16, page 875, "Given the changes in society, as well as the enforcement mechanisms that exist today, particularly given the FTC's new focus on "unfairness," and the well-recognized need to balance regulation and innovation, a different theoretical construct must be created—one that cannot be based upon precluding information sharing via common law methods. Instead, the overarching principle of privacy of today should not be the right to be let alone, but rather the principle of proportionality. This is Privacy 3.0."

[22] See, Preliminary Report, supra, note 12.

[23] See, Serwin, supra, note 16, pgs. 811-13, citing Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, pgs. iv, 3-6, Preliminary Staff Report, (2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf, last visited June 9, 2012.

[24] See, Serwin, supra, note 16, 852-53.

[25] Protecting Consumer Privacy in an Era of Rapid Change, supra, note 8, pgs. 58-60.

[26] Id., supra note 8, at pg. 20.

[27] Id., at pg. 9.

[28] Id., at pg. 47.

[29] Id., at pg. 50.

[30] Id., at pg. iv.

[31] Id., at pgs. 59-60.

[32] Id., at pg. 21, fn. 109.

[33] Id., at pg. 30.

[34] Id., at pg. 47.

[35] Id., at pgs. 59-60.

[36] See, Serwin, supra, note 16, citing Ann Cavoukian, The 7 Foundational Principles, Privacy by Design (Jan. 2011), http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

[37] Id.

[38] Id., at pg. 59.