Monday, October 1, 2012
11:00 AM - 12:30 PM

701 – Social Media Risk & Responsibility in the Use of Health Care Technology

Kenny Johnson
Senior Corporate Counsel
Quest Diagnostics Incorporated

Linda Kearney
Managing Senior Associate General Counsel
Wellpoint, Inc.

Kimberley Overs
Assistant General Counsel
Pfizer, Inc.

Andy Serwin
Chair: Privacy Security and Information Management Practice
Foley & Lardner LLP

Faculty Biographies

Kenny Johnson

Kenneth Johnson is senior corporate counsel for the AmeriPath division of Quest Diagnostics Incorporated, the world's leading provider of diagnostic testing, information and services. In this role, Mr. Johnson provides legal support to senior management, medical professionals, and the sales and marketing functions on numerous issues concerning the anatomic pathology, dermatopathology, and molecular diagnostic services provided by the division.

Prior to this role, Mr. Johnson served as senior corporate counsel-legal and compliance, responsible for advising management on various federal and state health care fraud and abuse laws, physician self-referral issues, Medicare and other third-party reimbursement issues, and data privacy and security matters. With Quest Diagnostics, he also served as director, legal compliance, compliance attorney, and director, employee relations.

He currently serves as past-president of the ACC's Dallas-Fort Worth Chapter and has been a board of director member since 2006. Mr. Johnson also serves as Pack Committee chair for the local BSA troop and serves as lay leader for Fellowship United Methodist Church.

Mr. Johnson received his undergraduate degree from Louisiana State University, and earned his law degree from the Paul M. Hebert Law Center at Louisiana State University. He was a member of the *Law Review* and graduated Order of the Coif.

Linda Kearney

Linda M. Kearney is managing senior associate general counsel in the litigation for WellPoint, Inc., and serves on WellPoint's litigation management team. Her primary responsibilities are to manage significant provider litigation, provide litigation/risk management advice on provider related issues and to oversee all litigation nationwide for UniCare/HealthLink. She was the team leader for the company's first outside counsel convergence initiative for litigation.

Prior to joining WellPoint, Ms. Kearney was a partner at the law firm of Porter, Rogers, Dahlman & Gordon, P.C., in Corpus Christi, TX, and served as assistant attorney general in the law enforcement defense division of the Texas attorney general's office.

She helped form the ACC's Health Law Committee and is chair. She also serves on the ACC's Austin Chapter board of directors and has held a variety of positions for the chapter. Linda was previously the secretary and vice-chair of the ACC's Litigation Committee. She regularly speaks on litigation and outside counsel management topics. She is actively involved as an adult leader for cub scouts and boy scouts.

Ms. Kearney holds a JD from the University of Notre Dame Law School and a BA in philosophy from The George Washington University. She has been board certified in civil trial law by the Texas board of legal specialization since 1998.

Kimberley Overs

Kimberley Danzi Overs is assistant general counsel at Pfizer, Inc. where her practice focuses on emerging channels. Ms. Overs serves as U.S. privacy lead for Pfizer's global privacy office and is a member of the board of the International Pharmaceutical Privacy Consortium.

Previously, Ms. Overs was vice president and legal counsel for the Estee Lauder Companies where she was responsible for the support of global new media initiatives, CRM marketing programs and privacy compliance. She also served as assistant general counsel and director of business affairs for Audible.com, a provider of spoken-word digital audio. Ms. Overs was a litigator for Fried, Frank, Harris, Shriver & Jacobson LLP and Hughes, Hubbard, & Reed LLP.

Ms. Overs is the present chair of the IT, Privacy and eCommerce Committee. She is also chair of the Alumnae of Columbia Law School.

Ms. Overs holds an LLM from Columbia Law School and was awarded her JD by the State University of New York at Buffalo School of Law. She earned her BA at the University of Virginia.

Andy Serwin

Andrew B. Serwin is the founding chair of the privacy, security, and information management practice, and Foley's consumer protection practice, and is a partner in the San Diego and Washington, D.C., office of Foley & Lardner LLP. He also is the executive director of the Lares Institute, a think tank that focuses on emerging technology and information governance issues. Mr. Serwin has handled a number of high-profile privacy matters before the Federal Trade Commission, ranked second on Computerworld's list of "Best Individual Privacy Advisers", and was named to *Security Magazine's* "25 Most Influential Industry Thought Leaders" for 2009, where he is the only law firm lawyer to receive this award. He is also ranked by Chambers USA - 2009-2011 in the area of National: Privacy & Data Security. He is the author of *Information Security and Privacy: A Guide to Federal and State Law and Compliance*, which has been called "the best privacy sourcebook", and "an indispensible resource for privacy professionals at all levels".

The Lares Institute

Social Media: Understanding User Patterns and Compliance Issues

June 2011

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Lares Institute is pleased to present the results of *Social Media: Understanding User Patterns and Compliance Issues.* This study examines use patterns of social media, the nature and extent of disclosure of information via social media, and the role of corporate policies and policies on social media platforms.

Social media has quickly become a central component of many people's lives. While it can be a tool for personal enjoyment, social media has become a big business and many companies are attempting to reach the audiences that social media platforms have quickly garnered. The goals of the study were to determine: the nature and extent of social media use for business versus personal use; which social media platforms were used for business versus personal use; gather certain information regarding use patterns with social media, particularly regarding the nature and extent of "friending"; individuals' attitudes regarding disclosures via social media; as well as the level of review of corporate polices and social media privacy policies.

The Lares Institute sent surveys to 802 individuals in the United States, and received 741 responses. The following is a summary of highlights from the study on social media:

- The overwhelming majority of those surveyed use some form of social media. However, significantly more people use social media for personal use than for business use.

- Facebook, YouTube, and LinkedIn were identified as the most popular social media services overall.

- Facebook and LinkedIn are ranked as the most used social media service for business purposes.

- Facebook easily takes the lead as the most popular social forum when it comes to personal use. On the other hand, the once popular MySpace received one of the lowest usage response rates of all social media services included in the survey.

- Social media services have seemingly developed a new trend wherein people are accustomed to being "friends" without ever having met.

- Generally, social media users believe that people voluntarily disclose too much information online. Moreover, a majority of social media users are at least minimally concerned about online privacy.

- When it comes to compliance policies, only a minority of users actively read the details of social media service policies before accepting.

- Corporate use of social media is rising—49% of respondents report that their employer uses social media to promote its products or services. While almost 52% of respondents were aware of a corporate social media use policy, almost 48% reported that their employer either didn't have a policy, or they were unaware of a policy existing.

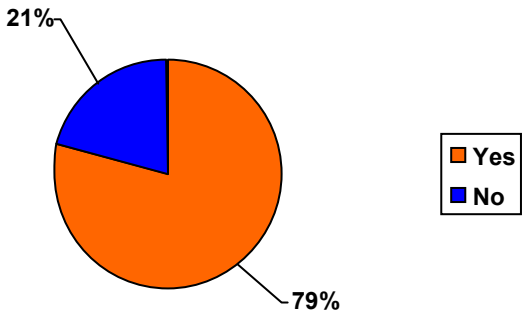
II. KEY FINDINGS OF THE SURVEY

The survey focused on use patterns and compliance issues with social media. The following section presents the findings of the survey, with accompanying graphical representations of the results.

Who uses social media?

Out of approximately 800 survey participants, 79% use some form of social media, while 21% do not utilize social media services.

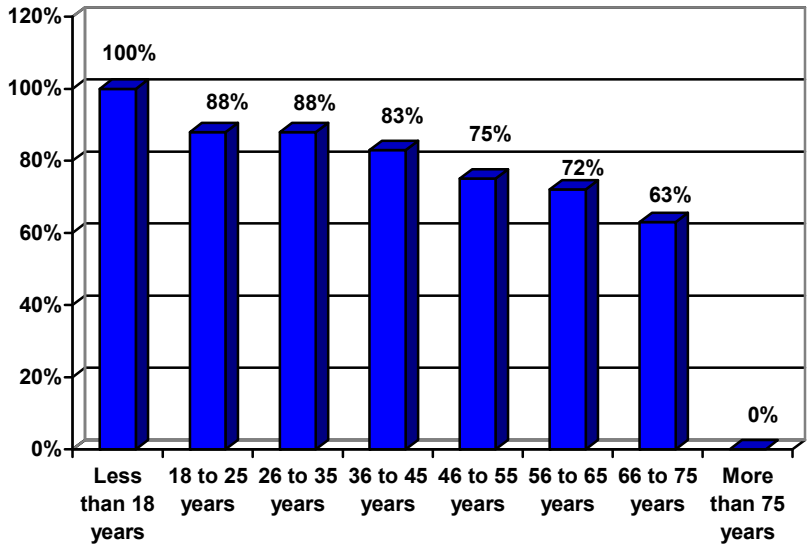
Chart 1:
Q. Do you use social media?



Social Media Use by Age

One area where there was a statistically significant variance in the data was when social media use was examined against the age of the respondent. Not surprisingly, younger people reported higher social media use than older respondents.

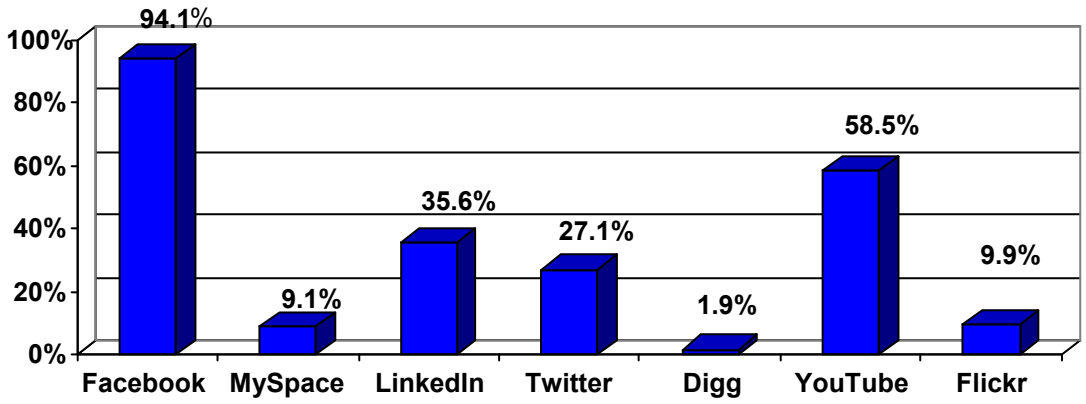
Chart 2:



What are the most commonly used forums of social media?

Facebook's market position was confirmed by this survey. Social media juggernaut Facebook was reportedly used by 94% of the respondents while YouTube received the second highest response rate, at 58%, LinkedIn followed at 35.6%. Beyond this, Flickr, Digg, and MySpace received significantly lower usage rates in comparison to other social media services as is seen below.

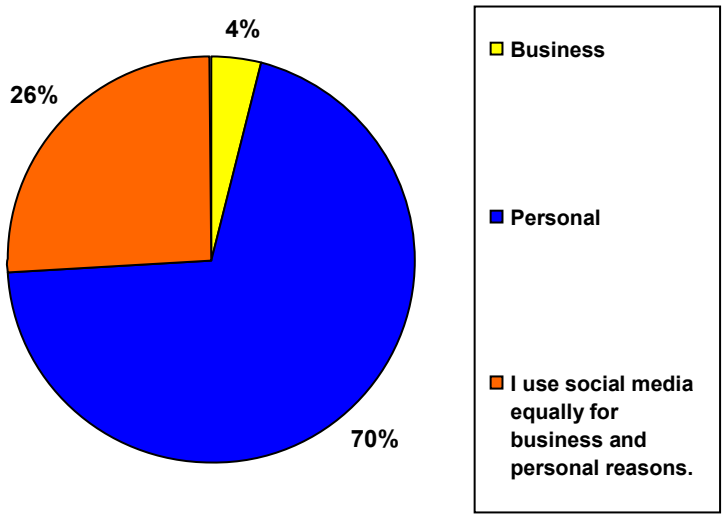
Chart 3:
Q. What forms of social media do you use?



A. Social Media: Business Use

Chart 4 reveals that only 4% of survey participants primarily use social media for business, while 26% reported that they use social media equally for both personal and business purposes.

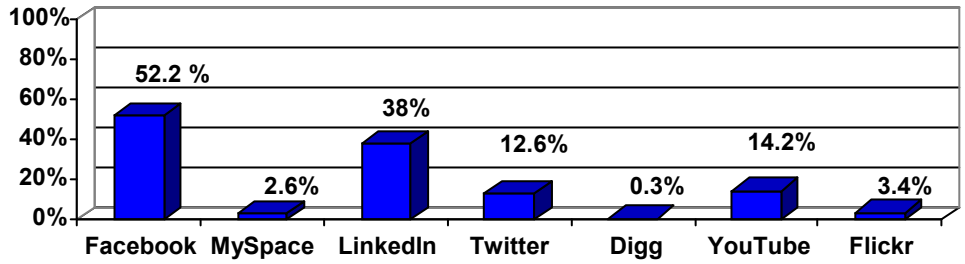
Chart 4:
Q. What is your primary reason for using social media?



What are the most commonly used social media forums in business?

Chart 5 displays Facebook and LinkedIn as the most popular forms of social media to utilize in business among study participants.

Chart 5:
Q. Which social media services do you use primarily for business purposes?

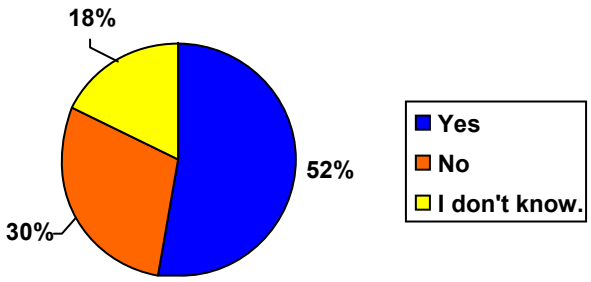


Do companies maintain policies regarding the use of social media at their place of business?

Since social media presents the opportunity for rapid dissemination of information, one area that can present risk to companies is the unregulated use of social media in the workplace. Approximately half of survey participants indicated that they were aware that their company has policy regarding the use of social media in the workplace.

Chart 6:

Q. Does your employer have a policy regarding the use of social media?

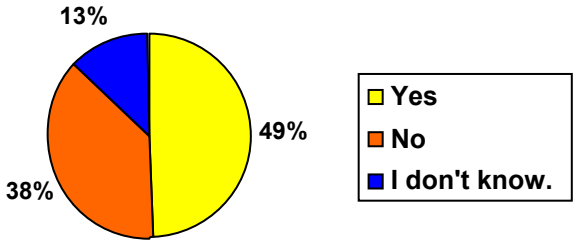


How often is social media used as a marketing tool?

Chart 7 shows that approximately half of survey participants are aware that their employer uses social media as a marketing tool to promote their business.

Chart 7:

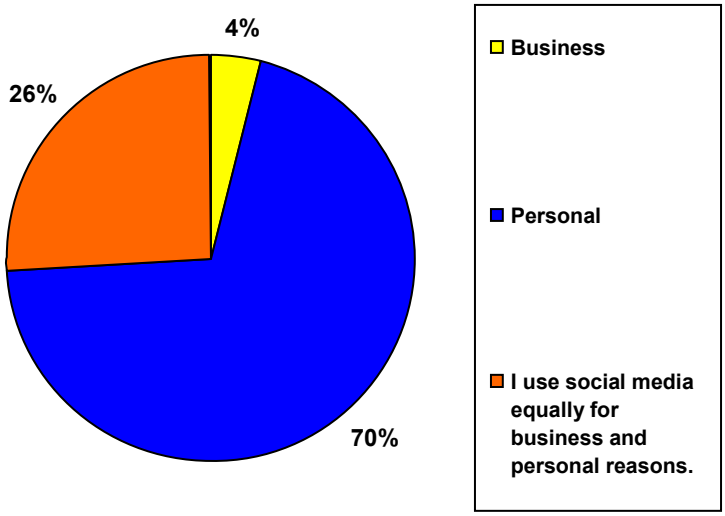
Q. Does your employer use social media to promote its products or services?



B. Social Media: Personal Use

Chart 8 reveals that 70% of survey participants primarily use social media for personal reasons, while 26% reported that they use social media equally for both personal and business purposes.

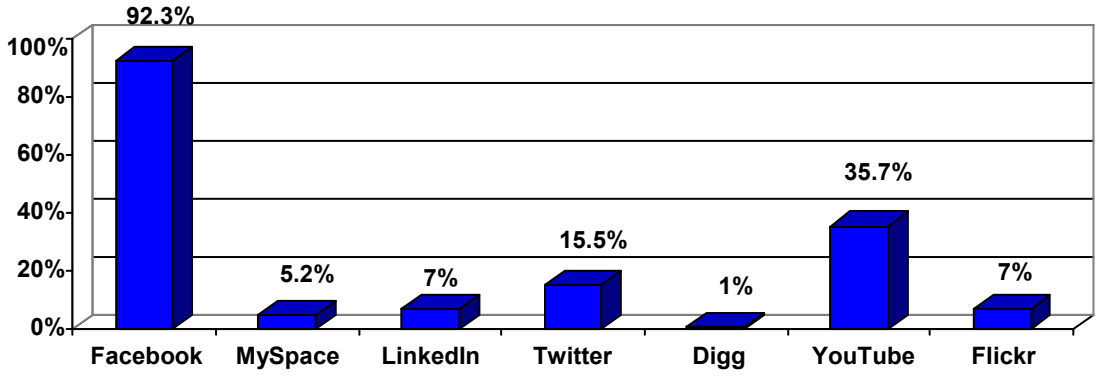
Chart 8:
Q. What is your primary reason for using social media?



What are the most popular social media forums used for personal reasons?

With a response rate of 92%, Facebook was the most utilized social media service for personal use. YouTube was chosen 36% of the time, while Twitter followed with a 16% usage rate among our survey participants.

Chart 9:
Q. Which social media services do you use primarily for personal reasons?



C. Social Media: Daily Use

Approximately half of this study's participants spend less than an hour a day using social media. However, 25% of participants indicated that they spend at least two or more hours a day using some form of social media. Younger respondents also reported more social media use than their older peers.

Chart 10:
Q. How many hours per day do you use social media?

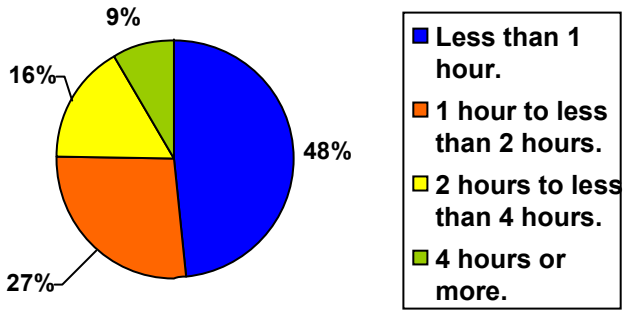
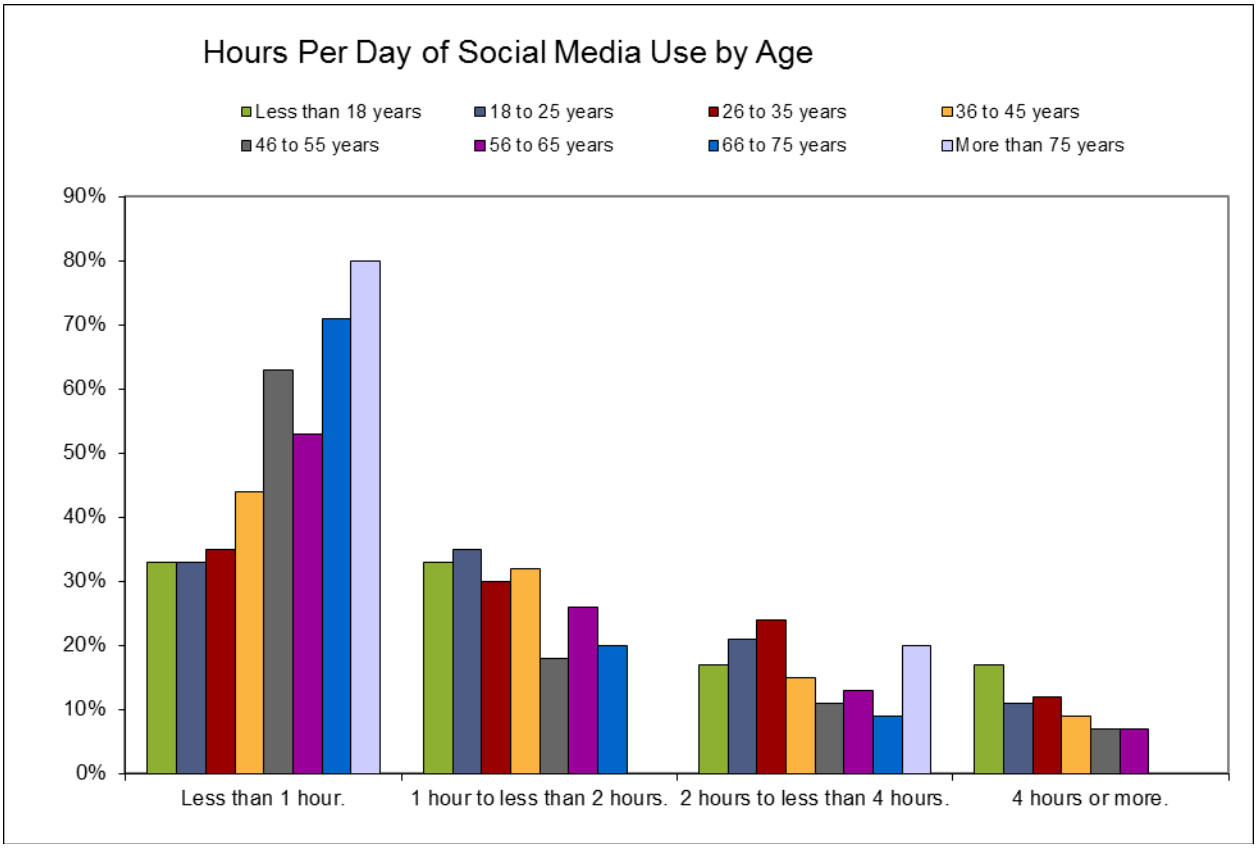


Chart 11:
Social Media Use by Age

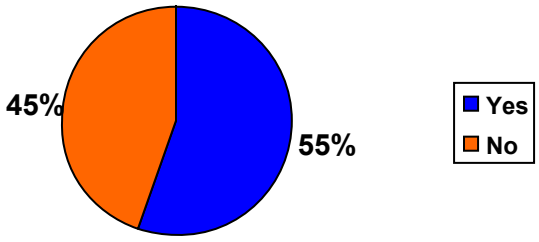


D. Social Media: "Unmet Friends"

The concept of "friends" an individual has not met is a new phenomenon created by social media platforms. 55% of survey participant designated that they are personally acquainted with all of their social media friends. However, 45% indicated that they have social media friends that they have never met.

Chart 12:

Q. Do you have "friends" from social media you have never met?

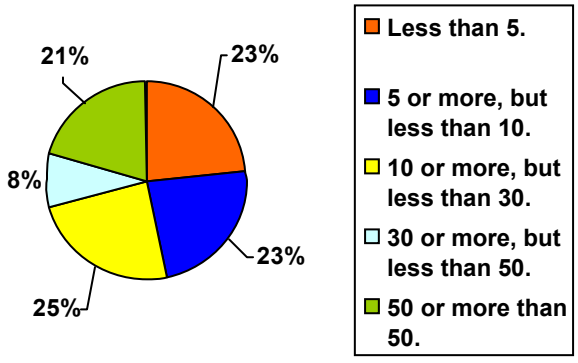


The majority of respondents who had "unmet friends," had a number of them. 23% had 5 or less friends they had not met. However, 8% had more than 30 friends, but less than 50 friends, they had not met. 21% had 50 or more than 50 friends they had not met.

One clear finding is that social media is changing the way people interact, particularly with people they do not know in the offline world.

Chart 13:

Q. How many "friends" do you have from social media that you have never met?



E. Social Media: Concern Over Privacy

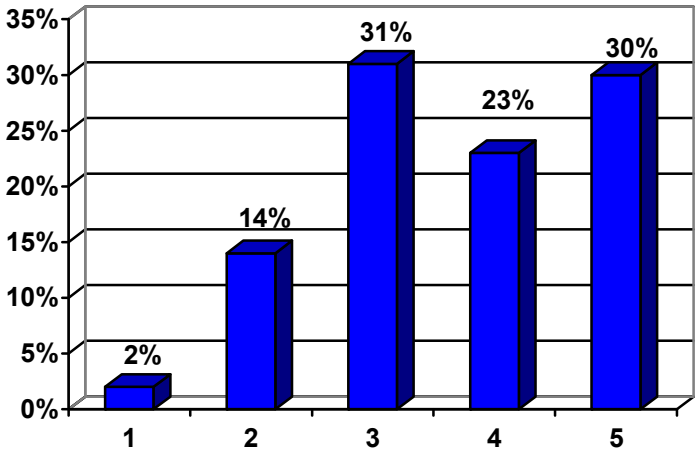
Individual concern over privacy is something that has gained significant media attention. Respondents were asked to rank themselves on a 1 to 5 scale with 1 being not concerned at all about privacy, and 5 being extremely concerned over privacy. 2% of respondents reported that they were not concerned at all about privacy, and ranked themselves at a "1". 14% ranked themselves as a 2, 31% as a 3, 23% as a 4, and 30% as a 5. The mean of the responses was 3.6382, and the median was 4.

There are a number of findings related to privacy sensitivity that will be the subject of future white papers, but two are worth noting. First, while age is a factor in privacy sensitivity, there are also other variables that correlate to privacy sensitivity. Second, while privacy sensitivity is somewhat predictive of certain behaviors, there are other variables that have strong correlations to certain other related behaviors as well.

Privacy Sensitivity

Chart 14:

Q. Please rate your personal concern over online privacy on a 1 to 5 scale, with 1 being not concerned at all about privacy and 5 being extremely concerned over privacy.



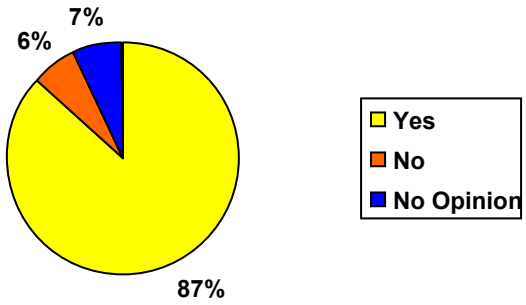
F. Social Media: Disclosure

How much is too much?

Another clear finding of the study is that people believe that there is too much voluntary disclosure of information on the internet. Chart 15 shows that the vast majority of survey participants (87%) believe that people voluntarily disclose too much information on the internet, while only 6% disagree.

Chart 15:

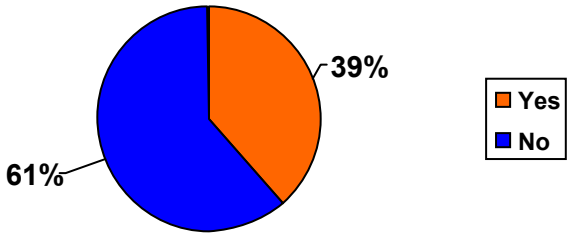
Q. Do you believe people disclose too much information voluntarily on the internet?



Additionally, only 39% of participants believe that inappropriate information has been disclosed about them online.

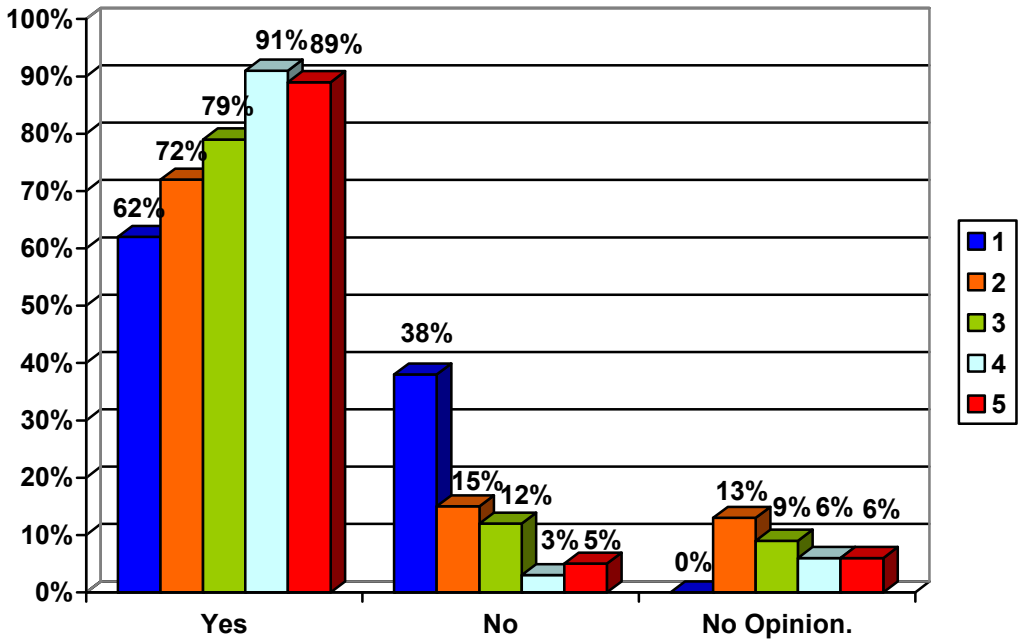
Chart 16:

Q. Has anyone posted information online about you that you felt was inappropriate?



Some other patterns emerge when the data is examined. Survey respondents were asked to rank their privacy sensitivity on a 1 to 5 scale, and those that reported they were more privacy sensitive, were more likely to believe that people disclosed too much information on the Internet.

Chart 17:
Voluntary Disclosures on the Internet / Privacy Sensitivity

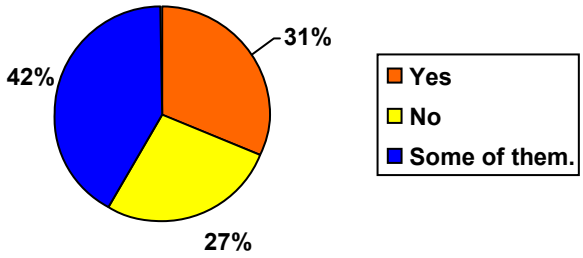


G. Social Media: Do People Read Privacy Policies?

Only 31% of survey participants affirmatively read social media privacy policies, while 27% of survey participants do not. 42% reported that they read some social media policies. There are some variables that impact who reads privacy policies that will be the subject of future white papers from the Lares Institute.

Chart 18:

Q. Have you read the privacy policies for the social media services you use?

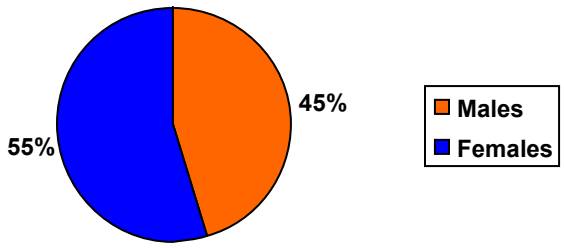


H. Survey Demographics

Gender:

Females comprised 55% of survey respondents, while Males comprised the remaining 45% of participants.

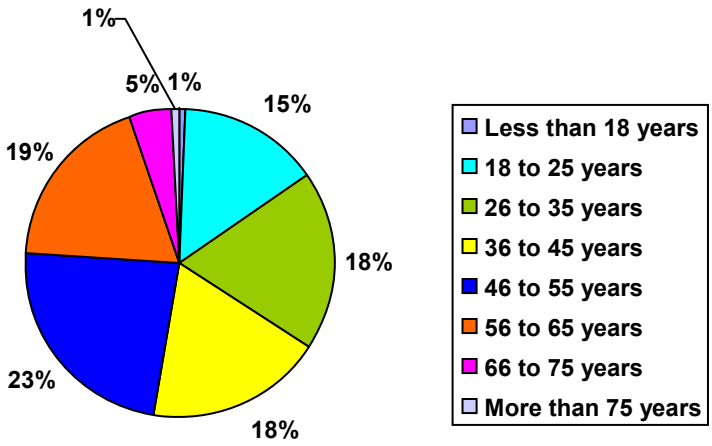
Chart 19:



Average Age:

Of those surveyed, 61% of social media users were between the age of 26 – 55. 23% of users were reported to be above the age of 56, while 16% were age 25 or below.

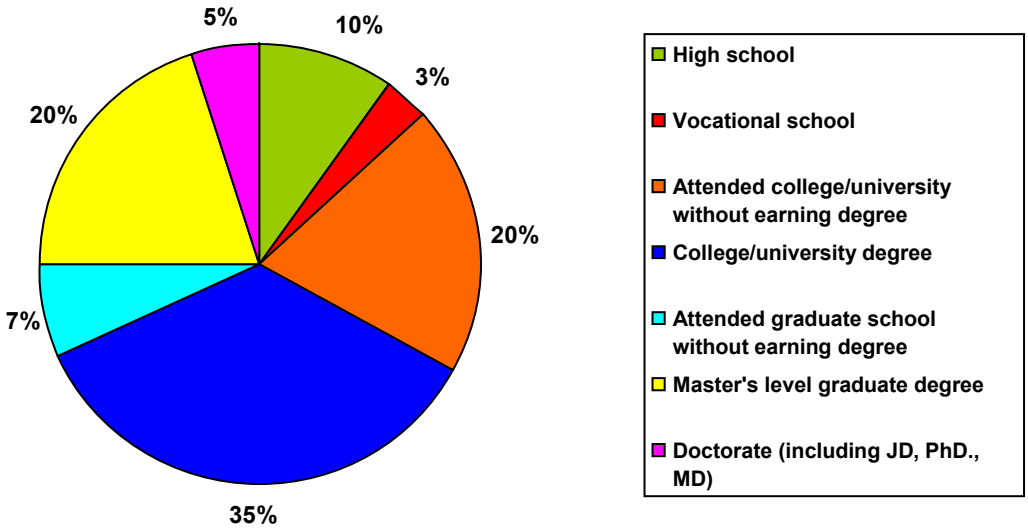
Chart 20:



Education:

The following percentages indicate the highest levels of education obtained by survey participants: Doctorate Degree → 5%; Masters Degree → 20%; Undergraduate Degree → 35%; High school → 10%.

Chart 21:

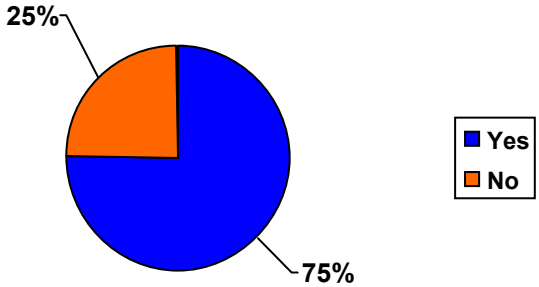


Employment:

The majority of survey participants were employed at the time of answering this survey.

Chart 22:

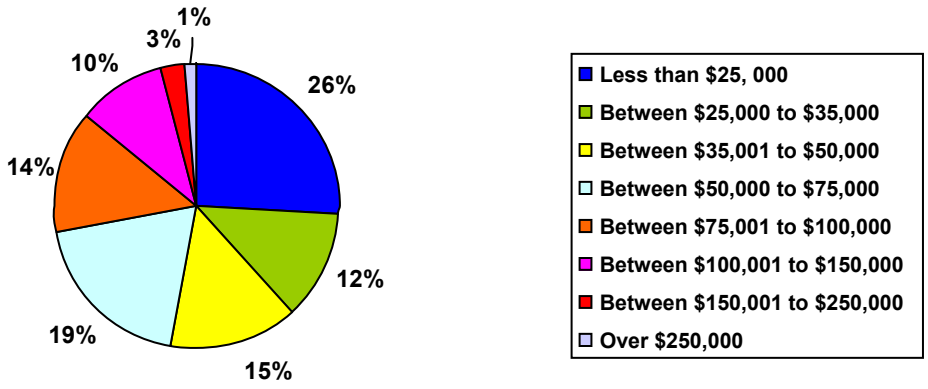
Q. Are you currently employed?



Average Income:

The income of survey participants spanned from 4% earning over $150k, 24% earning between $75k - $150k, 46% earning between $25k - $75k, and 26% earning below $25k.

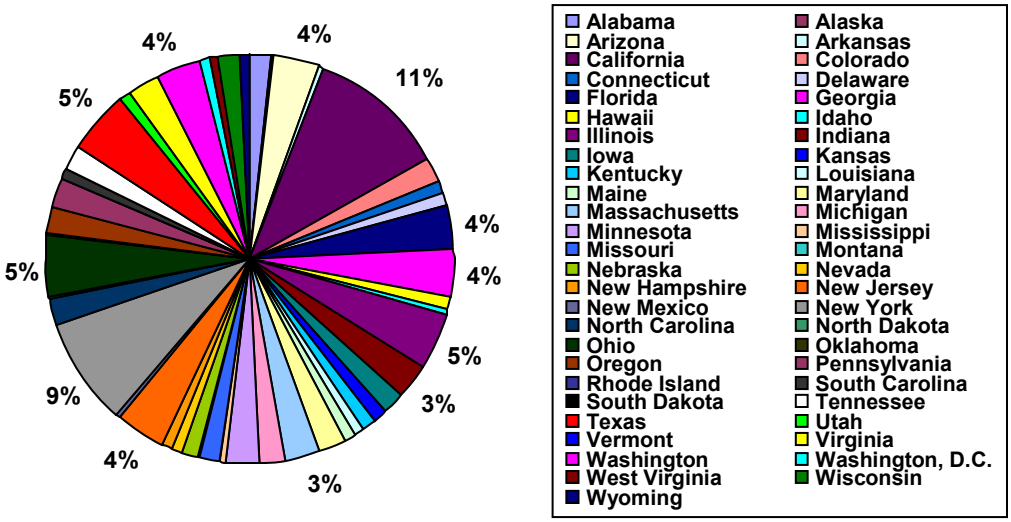
Chart 23:



Residence:

Survey participants largely reside in the following states: California →11%; New York → 9%; Texas → 5%; Illinois → 4.5%; Ohio →4.5%.

Chart 24:



III. SURVEY METHODS

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. The survey was sent to 802 individuals in the United States, and 741 responses were received, for a 92.4% response rate. The margin of error of this survey is 5% at a 99% confidence level.

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 that 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 respondents.

IV. CONCLUSION

While social media started as a way for people to communicate and stay in touch with people they know, it is becoming a key commercial venue for many companies to promote their goods and services. The rapid ascension of social media as a platform for personal and business interactions means that individuals and companies must be aware of the benefits and risks associated with social media. Individual users must also be aware of policies, whether they are corporate policies regarding use of social media, or the privacy policies of the platforms themselves. While the survey respondents felt that too much information was disclosed on the Internet, many had not read the policies that disclose how these platforms use and disclose their information, though these policies clearly bind the users and permit certain disclosures of information. In essence, this study suggests that while some have familiarized themselves with the rules of the road, others have not, and this can lead to unaccounted risks.

The study also provides some important information regarding the platforms of choice for social media, and the changing role of social media. Facebook has a significant lead in market share over its nearest competitors, but it remains to be seen whether business-focused LinkedIn can garner more significant market share for the business-users of social media.

Finally, the study demonstrates some significant changes in the nature of our social interactions. The concept of “friends” that you have never met is a concept that made little sense before social media captured our attention, but since a significant percentage of the respondents reported that they had over 50 “friends” they had never met, the concept of friendship, at least in the online world, appears to be an evolving one.

Social media platforms are changing the way people interact and this evolution in interactions creates both opportunities and risks that companies must consider and account for in their social media strategy. The evolution of interactions also is changing some very basic concepts of relationships, at least in the online world, and future studies will examine what effect, if any, these changes are having on offline interactions. While two companies—Facebook and LinkedIn currently have significant market positions, the relative position of these companies, or perhaps companies we have not yet heard of, is something to watch as the world of social media continues to change.

APPENDIX. DETAILED SURVEY FINDINGS

The Lares Institute independently conducted all research. All survey responses are provided in the following frequency or percentage frequency tables.

II. KEY FINDINGS OF THE SURVEY

Do you use social media?	
Answer Options	**Response Percent**
Yes.	78.8%
No.	21.2%

Social Media Use By Age	
Answer Options	**Response Percent**
Less than 18 years	100%
18 to 25 years	88%
26 to 35 years	88%
36 to 45 years	83%
46 to 55 years	75%
56 to 65 years	72%
66 to 75 years	63%
More than 75 years	0%

What forms of social media do you use?	
Answer Options	**Response Percent**
Facebook.	94.1%
MySpace.	9.1%
LinkedIn.	35.6%
Twitter.	27.1%
Digg.	1.9%
YouTube.	58.5%
Flickr.	9.9%

A. Social Media: Business Use

What is your primary reason for using social media?	
Answer Options	**Response Percent**
Business.	4.3%
Personal.	69.7%
I use social media equally for business and personal reasons.	26.0%

Which social media services do you use primarily for business purposes?	
Answer Options	**Response Percent**
Facebook.	52.2%
MySpace.	2.6%
LinkedIn.	38%
Twitter.	12.6%
Digg.	0.3%
YouTube.	14.2%
Flickr.	3.4%

Does your employer have a policy regarding the use of social media?	
Answer Options	**Response Percent**
Yes.	52.4%
No.	29.7%
I don't know.	17.9%

Does your employer use social media to promote its products or services?	
Answer Options	**Response Percent**
Yes.	49.1%
No.	38%
I don't know.	12.9%

B. Social Media: Personal Use

What is your primary reason for using social media?	
Answer Options	**Response Percent**
Business.	4.3%
Personal.	69.7%
I use social media equally for business and personal reasons.	26%

Which social media services do you use primarily for personal reasons?	
Answer Options	**Response Percent**
Facebook.	92.3%
MySpace.	5.2%
LinkedIn.	7.0%
Twitter.	15.5%
Digg.	1.0%
YouTube.	35.7%
Flickr.	7%

C. Social Media: Daily Use

How many hours per day do you use social media?	
Answer Options	**Response Percent**
Less than 1 hour.	48.3%
Less than 2 hours.	27.0%
Less than 4 hours.	16.1%
More than 4 hours.	8.6%

D. Social Media: “Unmet Friends”

Do you have "friends" from social media you have never met?	
Answer Options	**Response Percent**
Yes.	55.5%
No.	44.5%

How many "friends" do you have from social media that you have never met?	
Answer Options	**Response Percent**
Less than 5.	23.3%
Less than 10.	23.0%
10 or more, but less than 30.	24.5%
30 or more, but less than 50.	8.3%
50 or more than 50.	20.9%

E. Social Media: Concern Over Privacy

Please rate your personal concern over online privacy on a 1 to 5 scale, with 1 being not concerned at all about privacy and 5 being extremely concerned over privacy.	
Answer Options	**Response Percent**
1.	2.4%
2.	13.6%
3.	31.4%
4.	22.8%
5.	29.9%

F. Social Media: Disclosure

Do you believe people disclose too much information voluntarily on the Internet?	
Answer Options	**Response Percent**
Yes.	86.7%
No.	6.3%
No opinion.	6.9%

Has anyone posted information online about you felt was inappropriate?	
Answer Options	**Response Percent**
Yes.	38.6%
No.	61.4%

Voluntary Disclosure on the Internet / Privacy Sensitivity			
Answer Options → ↓	**Yes**	**No**	**No Opinion**
1	62%	38%	0%
2	72%	15%	13%
3	79%	12%	9%
4	91%	3%	6%
5	89%	5%	6%

G. Social Media: Do People Read Privacy Policies?

Have you read the privacy policies for the social media services you use?	
Answer Options	**Response Percent**
Yes.	31.3%
No.	26.9%
Some of them.	41.8%

H. Survey Demographics

What is your gender?	
Answer Options	**Response Percent**
Male.	45.3%
Female.	**54.7%**

What is your age?	
Answer Options	**Response Percent**
Less than 18 years	0.8%
18 to 25 years	14.7%
26 to 35 years	18.6%
36 to 45 years	18.5%
46 to 55 years	**23.5%**
56 to 65 years	18.5%
66 to 75 years	4.7%
More than 75 years	0.7%

Please check the range that best describes your highest education level.	
Answer Options	**Response Percent**
High school	10.1%
Vocational school	3.2%
Attended college/university without earning degree	19.7%
College/university degree	**35.1%**
Attended graduate school without earning degree	6.7%
Master's level graduate degree	20.1%
Doctorate (including JD, PhD., MD)	5.0%

Are you currently employed?	
Answer Options	**Response Percent**
Yes.	**75.2%**
No.	24.8%

Please check the range that best identifies your income.	
Answer Options	**Response Percent**
Less than $25,000	25.8%
Between $25,000 to 35,000	12.4%
Between $35,001 to 50,000	14.7%
Between $50,001 to 75,000	19.2%
Between $75,001 to 100,000	13.8%
Between $100,001 to 150,000	9.9%
Between $150,001 to 250,000	3.0%
Over $250,000	1.3%

Where in the U.S. do you reside?		
Answer Options	**Response Percent**	**Response Count**
Alabama.	1.6%	12
Alaska.	0.4%	3
Arizona.	3.6%	27
Arkansas.	0.5%	4
California.	**10.7%**	**79**
Colorado.	2.0%	15
Connecticut.	1.2%	9
Delaware.	0.8%	6
Florida.	3.5%	26
Georgia.	3.6%	27
Hawaii.	0.8%	6
Idaho.	0.7%	5
Illinois.	4.5%	33
Indiana.	2.7%	20
Iowa.	1.6%	12
Kansas.	1.1%	8
Kentucky.	1.2%	9
Louisiana.	0.9%	7
Maine.	0.7%	5
Maryland.	2.2%	16
Massachusetts.	2.8%	21
Michigan.	1.9%	14
Minnesota.	2.7%	20
Mississippi.	0.4%	3
Missouri.	1.6%	12
Montana.	0.0%	0
Nebraska.	1.5%	11
Nevada.	0.9%	7
New Hampshire.	0.8%	6
New Jersey.	3.9%	29
New Mexico.	0.3%	2
New York.	8.5%	63
North Carolina.	2.0%	15
North Dakota.	0.3%	2
Ohio.	4.5%	33
Oklahoma.	0.5%	4
Oregon.	2.0%	15
Pennsylvania.	2.2%	16
Rhode Island.	0.1%	1
South Carolina.	0.9%	7
South Dakota.	0.0%	0
Tennessee.	1.9%	14
Texas.	5.1%	38
Utah.	0.8%	6
Vermont.	0.0%	0
Virginia.	2.3%	17
Washington.	3.8%	28
Washington, D.C.	0.7%	5
West Virginia.	0.5%	4
Wisconsin.	1.9%	14

Wyoming.	0.7%	5

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

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.

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.

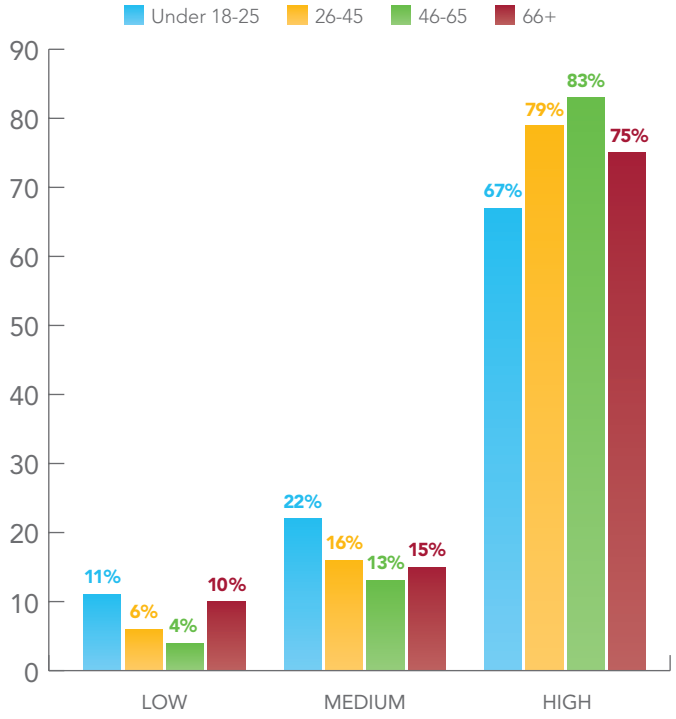
76. Information regarding criminal convictions
77. Instant message identifier
78. Information pertaining to service in the Armed Forces
79. Information regarding professional or employment history
80. Fax number
81. Information that reveals what hotels a respondent has stayed at
82. Place of birth
83. 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.

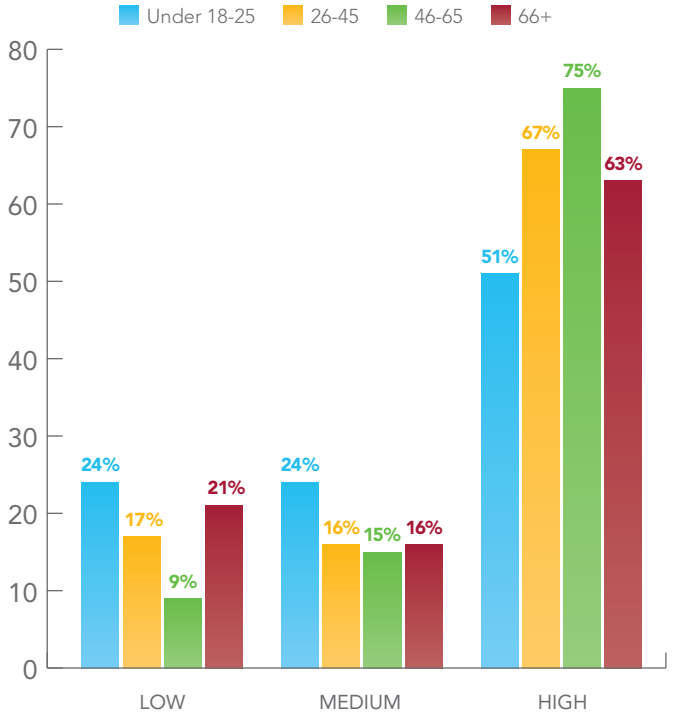
UNDERSTANDING PRIVACY SENSITIVITY

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.

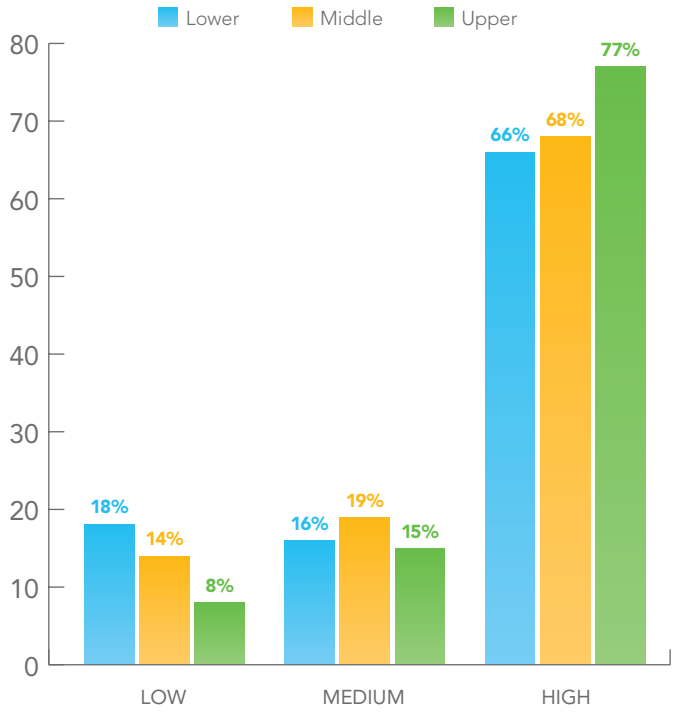
PRIVACY SENSITIVITY BY AGE



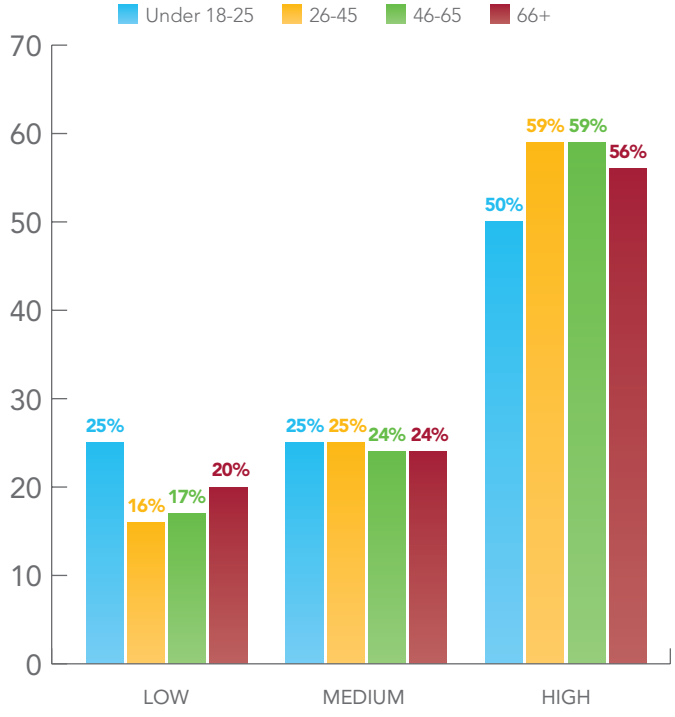
HEALTH INFORMATION SENSITIVITY BY AGE



HEALTH PRIVACY SENSITIVITY BY INCOME



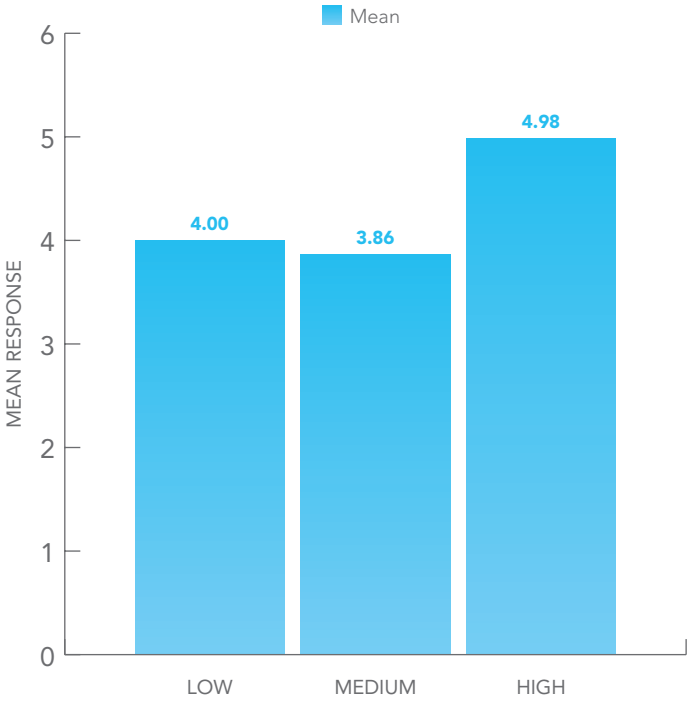
SOCIAL MEDIA PRIVACY SENSITIVITY BY AGE



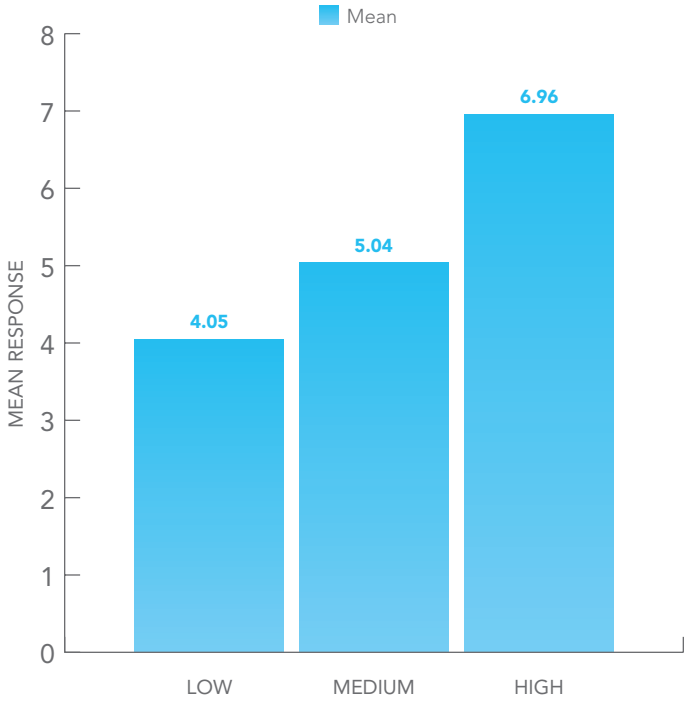
SELF-IDENTIFIED SENSITIVITY AND DATA-ELEMENT SENSITIVITY

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.

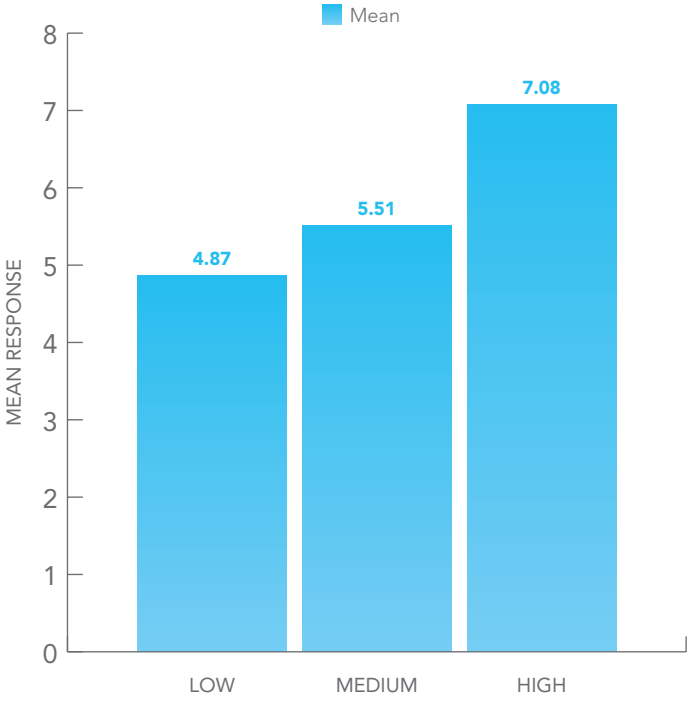
GAME DATA SENSITIVITY



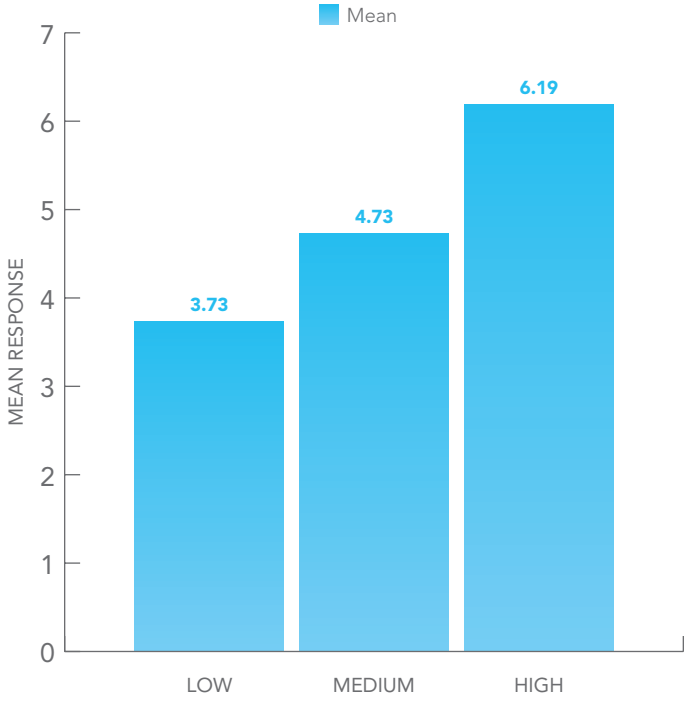
SOCIAL MEDIA SENSITIVITY

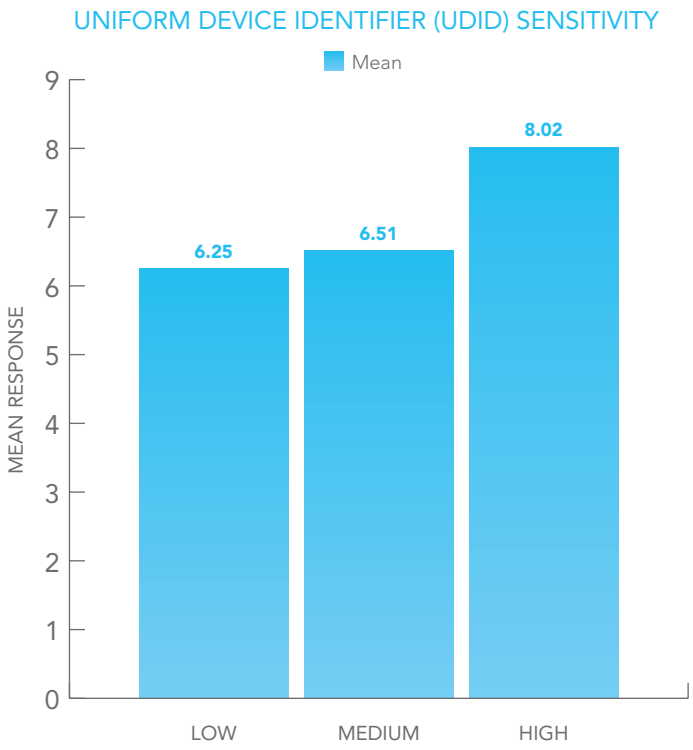


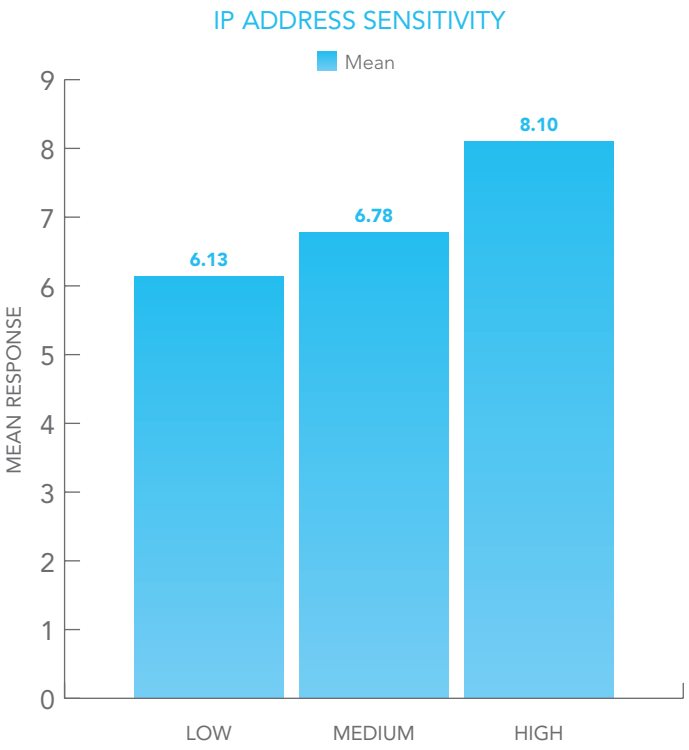
WEB HISTORY SENSITIVITY

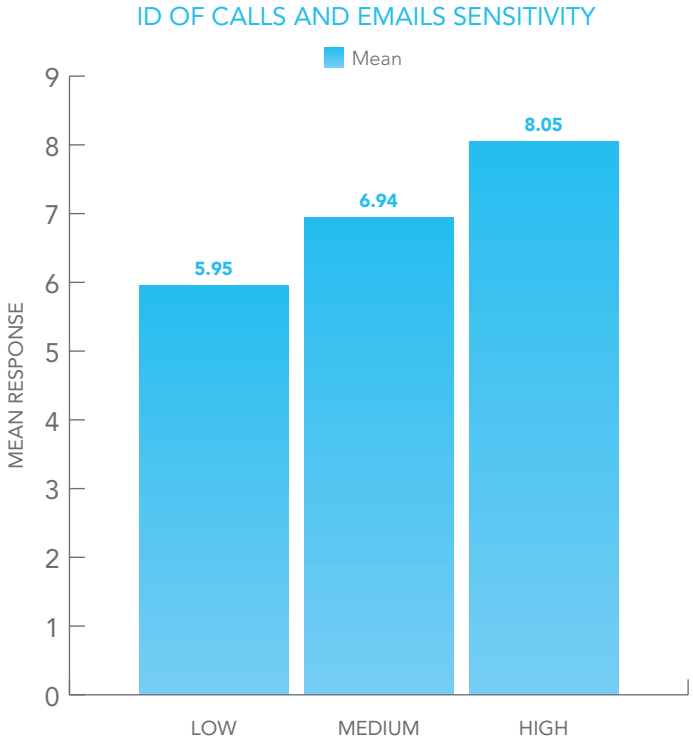


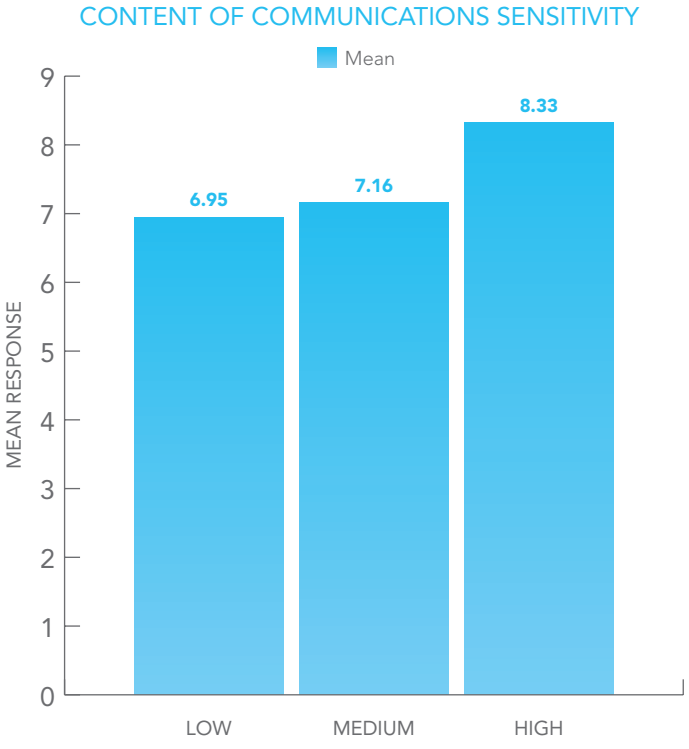
PURCHASE HISTORY SENSITIVITY







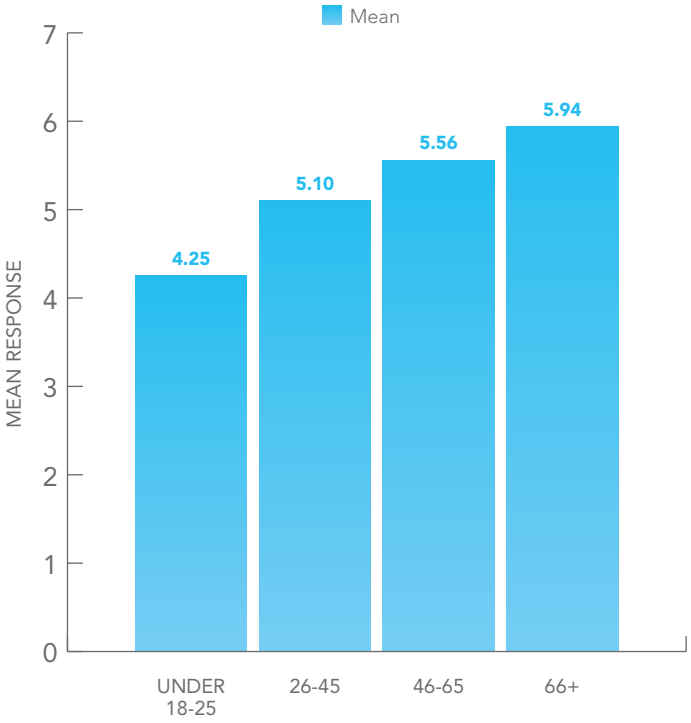




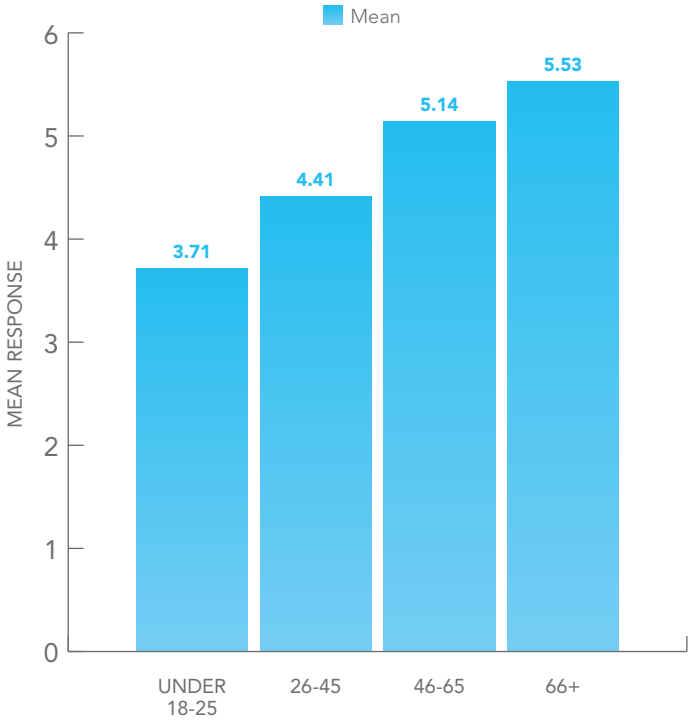
DEMOGRAPHICS AND DATA-ELEMENT SENSITIVITY

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

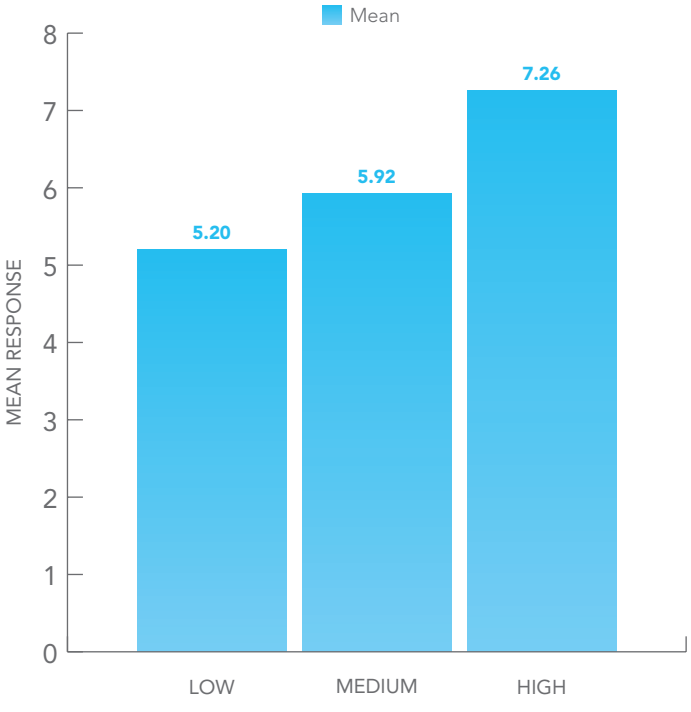
PURCHASE HISTORY AND AGE



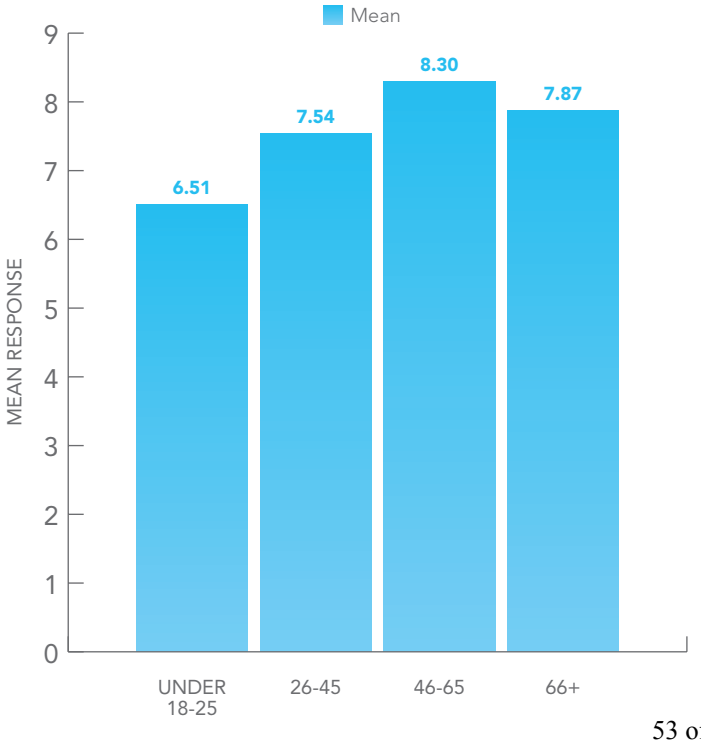
AGE AND LIKES



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.

The Lares Institute

The Demographics of Privacy—A Blueprint for Understanding Consumer Perceptions and Behavior.

September, 2011.

TABLE OF CONTENTS

I. Introduction

Privacy and information security is a fundamental business issue for companies, and as the most recent high-profile data breaches demonstrate, privacy mishaps can have a significant business impact, as well as lead to regulatory enforcement. Last year, the Federal Trade Commission released a report, "Protecting Consumer Privacy in an Era of Rapid Change: A proposed Framework for Businesses and Policymakers", in which the FTC suggested voluntary improvements to privacy practices. As noted by the opening sentences of the report:

> In today's digital economy, consumer information is more important than ever. Companies are using this information in innovative ways to provide consumers with new and better products and services. Although many of these companies manage consumer information responsibly, some appear to treat it in an irresponsible or even reckless manner. And while recent announcements of privacy innovations by a range of companies are encouraging, many companies – both online and offline – do not adequately address consumer privacy interests.[1]

This report had several recommendations for companies, including two of particular import—the adoption of "*Privacy by Design*" and providing consumers with greater choice regarding privacy.[2] This recommendation followed the landmark unanimous adoption of a resolution

[1] Protecting Consumer Privacy in an Era of Rapid Change: A proposed Framework for Businesses and Policymakers, (December 2010). The issues were further defined as follows: "Stakeholders emphasized the need to improve transparency, simplify the ability of consumers to exercise choices about how their information is collected and used, and ensure that businesses take privacy-protective measures as they develop and implement systems. At the same time, commenters and participants 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. Participants noted, for example, that the acquisition, exchange, and use of consumer 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."

[2] "First, companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy. Companies also should implement and enforce procedurally sound privacy practices throughout their organizations, including, for instance, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services. Such concepts are not new, but the time has come for industry to implement them systematically. Implementation can be scaled to each company's business operations. Companies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data, collect data of a sensitive nature, or engage in the business of selling consumer data.

Second, Commission staff proposes that companies provide choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past. Under this approach, consumer choice would not be necessary for a limited set of "commonly accepted" data practices, thus allowing clearer, more meaningful choice with respect to practices of greater concern. This component of the proposed framework reflects the concept that it

regarding PbD by the 32nd International Conference of Data Protection and Privacy Commissioners.[3]

The voluntary adoption of PbD offers companies an important solution to certain privacy concerns, and it is a well-documented approach to privacy which has the objectives of "…ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage…"[4] These objectives are implemented by 7 Foundational Principles, including:

> 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.[5]

Thus, in addition to permitting personal control of information, PbD explicitly recognizes that improved privacy practices can create a competitive advantage for businesses, *but this competitive advantage can only be realized if the changes businesses make as they implement PbD are perceived by consumers as adding value*.

In order to implement PbD in a way that maximizes its utility as a tool to drive best practices, research needs to be done to integrate consumer attitudes and behaviors into privacy designs. This research, if completed, would permit companies to design privacy in a way to permit consumers to gain control of their information, and permit companies to better anticipate and prevent privacy issues before they happen. In short—research needs to be done to create a blueprint for PbD.

---

is reasonable for companies to engage in certain commonly accepted practices – namely, product and service fulfillment, internal operations such as improving services offered, fraud prevention, legal compliance, and first-party marketing. Some of these practices, such as where a retailer collects a consumer's address solely to deliver a product the consumer ordered, are obvious from the context of the transaction, and therefore, consent for them is inferred. Others are sufficiently accepted – or necessary for public policy reasons – that companies need not request consent to engage in them. By clarifying those practices for which consumer consent is unnecessary, companies will be able to streamline their communications with consumers, reducing the burden and confusion on consumers and businesses alike." Protecting Consumer Privacy in an Era of Rapid Change:, pages v-vi.

[3] http://www.privacybydesign.ca/content/uploads/2011/02/2011-01-28-PbD-Toronto.pdf, page 17. Last visited August 12, 2011.

[4] http://privacybydesign.ca/about/principles/, last visited August 4, 2011. Dr. Ann Cavoukian, Ph.D, the Information & Privacy Commissioner of Ontario, Canada is the founder of PbD.

[5] http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf, last visited January 15, 2011.

While any single piece of research or article cannot hope to create this blueprint, this article does offer a starting point for further research, and for companies that want to better understand consumers' expectations regarding privacy. This study examines privacy from the individual perspective in two ways—it examines what people think about certain forms of privacy, and what they do about privacy, *i.e.* what steps they take to protect their privacy, and what privacy policies they read. This permits some examination of whether people who believe they are concerned about privacy actually are sufficiently concerned to change their behaviors. This article also offers some initial conclusions regarding consumer attitudes and behaviors, so that companies can better assess individual attitudes regarding privacy and incorporate these into PbD, or other information governance structures.

II. 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, and 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.

III. Executive Summary.

There are certain clear patterns that become apparent when demographic issues and privacy are examined. First, age is one of the most relevant factors to predict both privacy sensitivity, as well as privacy protective behavior, but it is not a linear relationship, and the 46-65 age range is consistently the most privacy sensitive and protective group. Second, in a somewhat surprising finding, education levels were generally inversely related to self-reported sensitivity, and education level was clearly inversely related to individuals' privacy protective behavior. Third, income overall was not that significant in predicting sensitivity, but had relevance to predicting privacy protective behavior in the sense that higher income individuals were generally less likely to read privacy policies.

Fourth, there was consistency between self-assessed privacy sensitivity and other responses in the survey. When the mean rankings of data elements are examined and compared to respondents' self-reported privacy sensitivity, as shown below, the respondents who self-assessed themselves as being more sensitive regarding health information also consistently ranked health-related data elements higher on the 1-10 scale in 13 of 14 cases.

Fifth, consumers do not always review privacy policies, but generally review them in a pattern consistent with certain common consumer agreements, and the relative review of these policies appears to relate to how sensitive consumers perceive the information at issue to be.

IV. Privacy Sensitivity.

One key issue the study examined is what were individuals' perceptions regarding privacy—specifically how sensitive they were to privacy issues generally, and also regarding certain key categories of information. The results of the questions are discussed in general, and this data was examined for patterns based upon demographic categorization.

A. Privacy Sensitivity Generally.

Respondents were first asked about how sensitive they were generally about privacy:

Table 1.

Privacy Sensitivity	Total
Low	6%
Medium	15%
High	79%

There were no statistically significant results when these results were examined based upon income or age categorizations. However, when age was considered, there were some strong correlations between age and general privacy sensitivity, with those in the under 18-25 category having the lowest sensitivity at 67% in the high category, 79% in the 26-45 category self-identifying as having high privacy sensitivity, and 83% in the 46-65 category reporting they were highly sensitive to privacy generally. Additionally, at the Medium level, there was a statistically significant correlation between Under 18-25, versus 46-65. Thus, while there was a statistically significant correlation between being in the 46-65 and 26-45 categories, when compared to the youngest category, there was not a statistically significant correlation between the 66+ category and the Under 18-25 category. Moreover, in the Low sensitivity category, 66+ was almost the same as the Under 18-25 category, and the 66+ category was different in a statistically significant way from 46-65.

Table 2.

Age

Privacy Sensitivity	Under 18-25	26-45	46-65	66+
Low	11%	6%	4%	10%
Medium	22%	16%	13%	15%
High	67%	79%	83%	75%

This result was confirmed when individual data elements were examined. As part of the survey, respondents were asked to rank the sensitivity of 100 data elements. When the mean score of each age cohort is examined, the 46-65 cohort had the highest mean ranking 68% of the time, the second highest 27% of the time, the third highest 5% of the time, and never was below the third highest mean ranking for any data element. Thus, the general finding that 46-65 has the highest sensitivity to privacy also appears when respondents were asked to rank individual data elements, which provides further validation for the conclusion that for privacy sensitivity generally, age is a predictor of privacy sensitivity, but it is not a direct linear relationship, as the 46-65 cohort was the most sensitive to privacy.

B. Privacy Sensitivity--Health.

For health sensitivity, demographic information was of more relevance. As a general matter, the respondents reported their sensitivity regarding health information as follows:

Table 3.

Privacy Sensitivity--Health	Total
Low	15%
Medium	17%
High	68%

A response that someone was sensitive to health information showed a remarkable correlation to how respondents ranked the sensitivity of the health data elements when they were asked to rank the sensitivity of these data elements. Of the 100 data elements respondents were asked to rank, 14 were health-specific and if the mean sensitivity rankings of these elements is examined, a clear pattern emerges. The 14 health elements were examined by taking each sensitivity grouping—general, financial, health, and social media—and comparing the mean value for each group that self-identified as having high sensitivity regarding each category. Those that self-identified as highly sensitive regarding health information consistently ranked health information as more sensitive than those who were sensitive regarding other forms of information. This group had the highest mean value for the data elements in 13 of the 14 data elements, which demonstrates that respondents' general self-assessment strongly correlates to data sensitivity when individual data elements are examined.

Moreover, people who had a higher income were more sensitive regarding their health information than those at a lower income level, and this was the most predictive of health privacy sensitivity.

Table 4.

Income

Privacy Sensitivity--Health	Lower	Middle	Upper
Low	18%	14%	8%
Medium	16%	19%	15%
High	66%	68%	77%

This conclusion was also seen when the 14 health data elements were examined. In each case, those with the highest income ranked the health data elements as more sensitive than those with a lower income.

Age was also predictive of privacy sensitivity, though it was not a direct linear relationship, with those in the 46-65 category being the most sensitive.

Table 5.

Age

Privacy Sensitivity--Health	Under 18-25	26-45	46-65	66+
Low	24%	17%	9%	21%
Medium	24%	16%	15%	16%
High	51%	67%	75%	63%

This conclusion was confirmed when the health data elements were examined, with those in the 46-65 category ranking the 14 health elements as the most sensitive 11 times, compared to other age groups. This is consistent with the finding that while being in this age cohort is predictive of sensitivity regarding health information, income had a stronger correlation to health information sensitivity.

Education level was also inversely predictive of health privacy sensitivity, with those who did not have a college degree being more sensitive regarding health information, with those who had a college or graduate degree being less sensitive in so far as less respondents in this cohort reported being highly sensitive than those without a college degree.

Table 6.

Education

Privacy Sensitivity--Health	No College Degree	College Degree or Graduate Degree
Low	14%	16%
Medium	14%	18%
High	72%	66%

In conclusion, age again was predictive of health sensitivity, with the 46-65 cohort being the most sensitive, but income was the most relevant factor to consider for health privacy sensitivity. As we will see in other areas, a higher education level was predictive of a lower sensitivity to health privacy.

C. Privacy Sensitivity--Financial.

Financial information was the category that respondents were the most sensitive about, with 90% reporting that they were highly sensitive regarding financial information.

Table 7.

Privacy Sensitivity--Financial	Total
Low	5%
Medium	5%
High	90%

From a demographic perspective, age was the only factor that was predictive of financial privacy sensitivity, with the 46-65 cohort again being the most sensitive.

Table 8.

Age

Privacy Sensitivity--Financial	Under 18-25	26-45	46-65	66+
Low	8%	4%	4%	8%
Medium	9%	5%	4%	6%
High	83%	91%	92%	86%

D. Privacy Sensitivity--Social Media.

Finally, respondents were asked to self-assess their privacy sensitivity regarding social media. Overall, respondents were generally less sensitive regarding social media privacy, with 58% falling into the "high" category, compared to 90% with financial privacy.

Table 9.

Privacy Sensitivity--Social Media	Total
Low	18%
Medium	24%
High	58%

Income and education were not predictive of sensitivity regarding this issue, and age was only predictive in a limited way. 25% of respondents in the under 18-25 category, compared to 16% in the 26-45 cohort self-reported as having a low sensitivity regarding social media privacy.

Table 10.

Age

Privacy Sensitivity--Social Media	Under 18-25	26-45	46-65	66+
Low	25%	16%	17%	20%
Medium	25%	25%	24%	24%
High	50%	59%	59%	56%

In sum, generally people were less concerned about social media privacy, and contrary to some popular belief, younger respondents were not significantly less concerned about social media privacy than other age-ranges.

E. Demographics and Privacy Sensitivity--In Summary.

Conclusions can be drawn regarding privacy sensitivity and demographic information that demonstrate there are certain correlations. Age is one of the most important factors in determining privacy sensitivity, but the relationship is not a directly relational one in the sense that higher age does not predict higher sensitivity. Instead, we consistently see that one age range, 46-65 is the most sensitive to privacy, with those younger, and older, being less sensitive. Income was slightly predictive of privacy sensitivity as it had a significant impact on health privacy sensitivity, but it had no other statistically significant correlation to privacy sensitivity.

Education level, where it was relevant, had an inverse relationship to privacy sensitivity, which is a result we will see replicated in other data. Finally, the belief that younger people "cared less" about privacy in social media is not supported by these results. While younger people self-assessed as being less sensitive to social media privacy issues than older respondents, there was not a statistically significant variance based upon age.

V. Demographics and Privacy Protective Behavior.

Another way to examine privacy and demographic issues is to analyze certain privacy protective behaviors and examine if there are any demographic correlations. While as noted above, certain age groups are more sensitive to privacy issues, that did not necessarily translate to a correlation in privacy protective behavior.

Respondents were asked a number of questions that related to privacy and information security protective activities, which were based in part upon the FTC's recommendations for consumers to avoid identity theft.[6]

A. Social Security Cards.

The first question respondents were asked was whether they carried their Social Security card in their wallet. Overall, 27% did and 73% did not.

Table 11.

	Total
Yes	27%
No	73%

There was not a statistically significant variance in these numbers based upon income, though higher income people tended to carry their Social Security number card less than lower and middle income respondents.[7]

[6] http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.shtm, last visited August 7, 2011.

[7] Education level was not predictive of this behavior.

Table 12.

Income

	Lower	Middle	Upper
Yes	28%	30%	21%
No	72%	70%	79%

However, age was predictive of whether people carried their Social Security card in a way that was surprising given the results of the questions regarding privacy sensitivity. The least privacy sensitive group—Under 18-25 carried their Social Security card in their wallet much less than the older groups, which were all more privacy sensitive than the youngest group.

Table 13.

Age

	Under 18-25	26-45	46-65	66+
Yes	14%	23%	31%	45%
No	86%	77%	69%	55%

B. Virus Protection.

Respondents were asked if they took steps to protect their computer from viruses and other security threats. Overall, 92% of respondents did take steps to protect their computer, and 8% did not. Education level was not significant for this question, but both income and age were important to consider. Upper income respondents protected their computer 97% of the time, compared to 89% of lower income respondents.

Table 14.

Total

Yes	92%
No	8%

Income

	Lower	Middle	Upper
Yes	89%	94%	97%
No	11%	6%	3%

In contrast to the question regarding Social Security numbers, age was predictive of whether people took steps to protect their computer from security threats, with older respondents taking steps more often than younger respondents.

Table 15.

Age

	Under 18-25	26-45	46-65	66+
Yes	78%	92%	95%	95%
No	22%	8%	5%	5%

C. Password Habits.

Respondents were also asked if they used information such as their mother's maiden name, their birth date, or the last four digits of their Social Security number as a password for their credit card, bank account or phone account. There were not statistically significant differences based upon an examination of demographic information, and overall 18% of people did use such information as their password, and 82% did not.

Table 16.

	Total
Yes	18%
No	82%

D. Verification of the Identity of Businesses.

Respondents were also asked whether they took steps to verify the identity and legitimacy of businesses that asked for PII, and overall 81% did, and 19% did not. There was a statistically significant variance based upon age, with only 69% of respondents who were in the under 18-25 age range responding that they did check this information, 85% of the 46-65 age demographic responding that they did check this information, and 90% of the 66+ age range verifying this information.

Table 17.

Total

Yes	81%
No	19%

Table 18.

Age

	Under 18-25	26-45	46-65	66+
Yes	69%	79%	85%	90%
No	31%	21%	15%	10%

E. Secure Storage of PII.

Respondents were asked if they kept PII in a secure location in their home, and overall 76% did, and 24% did not, and interestingly, people with no college degree were more likely to keep their information in a secure location than those that had a college or post-graduate degree.

Table 19.

Total

Yes	76%
No	24%

Education

	No College Degree	College Degree or Graduate Degree
Yes	83%	72%
No	17%	28%

F. Shredding of Information.

Respondents were asked if they shredded documents such as charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, or expired credit cards, before they threw them away. Overall, 58% did, 12% did not, and 30% did some of the time. Income was predictive of this behavior, but education level was, again in an inverse way, with 66% of those with no college degree shredding this information, compared to 54% of those with a college or graduate degree.[8]

Age was also predictive of this behavior, with 47% of those in the under 18-25 category shredding this information, 22% not shedding it, and 31% sometime shredding it, compared to 52%, 10% and 38% in the 26-45 category, and 64%, 11%, and 25% in the 46-65 category respectively.

[8] The impact of education level was the opposite when one considers the "sometimes" category.

Table 20.

Total

Yes	58%
No	12%
Sometimes	30%

Age

	Under 18-25	26-45	46-65	66+
Yes	47%	52%	64%	65%
No	22%	10%	11%	10%
Sometimes	31%	38%	25%	25%

G. Deposit of Mail.

A final question regarding whether respondents deposited mail in a secure location was asked. Overall, only 15% did, 63% did not, and 22% did some of the time. Here, income level was predictive of this behavior, with upper income respondents being more likely to deposit mail in a secure location. In contrast to some other areas, a higher education level was predictive of privacy protective behavior as respondents with a higher education level were less likely to use unsecure methods.[9]

Table 21.

Total

Yes	15%
No	63%
Sometimes	22%

Education

	No College Degree	College Degree or Graduate Degree
Yes	15%	16%
No	70%	59%
Sometimes	15%	25%

H. Conclusions.

Overall, the 46-65 cohort tends to be more privacy protective when these behaviors are examined, with the exception of the practice of carrying a Social Security card on their person. Higher income is somewhat predictive of privacy protective behavior, but higher education levels tend to have an inverse relationship to privacy protective behavior.

[9] While the use of secure mailing did not vary across education level, the failure to use it did—70% for those with a lower education level, compared to 59% of those with a higher education level, and this was also true for those that sometimes used secure mailing, with 15% of those without a college degree sometimes using secure mail, and 25% of those with a college or graduate degree sometimes using secure mail.

I. Do People Read Privacy Policies?

The final area that was examined regarding privacy-related conduct by individuals was whether people read privacy policies, particularly when the review of these documents in compared to other agreements individuals regularly enter. A number of questions regarding different types of privacy policies and other contracts are discussed below. It should be noted that the data is useful to examine in two ways. The raw numbers are helpful in the sense of understanding what people self-report about their review of agreements, and how demographic factors influence this issue. Perhaps as important is an analysis of the relationship between the numbers of people that self-report they review these documents is also helpful because it permits some conclusions to be drawn about the relative review of these documents in comparison to other commonly-enforced consumer transactions.

J. Review of Financial Privacy Policies.

Respondents were asked whether they read the privacy policies they received from their bank, credit card company, or other financial institution and 44% said they had read them, 12% said they had not reviewed them, and 44% had reviewed some of them.

Table 22.

	Total
Yes	44%
No	12%
Some of them	44%
I am unaware whether I receive these privacy policies	0%
I have not received any such policies	0%

Income level was inversely predictive of whether people read these policies, with 8% of middle income respondents saying they had not reviewed them, compared to 19% of upper income respondents who had not reviewed these policies.

Table 23.

Income

	Lower	Middle	Upper
Yes	45%	47%	34%
No	12%	8%	19%
Some of them	42%	45%	47%
I am unaware whether I receive these privacy policies	0%	0%	0%
I have not received any such policies	1%	0%	0%

Education level was also inversely predictive of whether people read these privacy policies, with 54% of people without a college degree reading these policies, compared to 39% of individuals with a college or graduate degree who read these policies.

Table 24.

Education

	No College Degree	College Degree or Graduate Degree
Yes	54%	39%
No	5%	16%
Some of them	41%	45%
I am unaware whether I receive these privacy policies	0%	0%
I have not received any such policies	1%	0%

K. Financial Privacy Policy Review--Conclusions.

With financial privacy policy review we see that income and education level were inversely predictive of policy review since individuals with higher incomes and higher education levels reviewed these policies less than individuals with lower incomes and education levels. Age was not predictive of financial privacy policy review.

L. Health Care Privacy Policy Review.

Overall, 52% of respondents read the privacy policies they received from their health care providers, 12% did not, and 35% read some of them. This number is higher than the financial privacy policy review and the highest number seen for privacy policy review.

Table 25.

	Total
Yes	52%
No	12%
Some of them	35%
I am unaware whether I receive these privacy policies	1%
I have not received any such policies	1%

As with financial privacy, both income and education level were inversely predictive of whether people read privacy policies. 56% of middle income respondents read these privacy policies, while only 41% of upper income respondents had read them.[10]

Table 26.

Income

	Lower	Middle	Upper
Yes	52%	56%	41%
No	11%	8%	22%
Some of them	35%	33%	37%
I am unaware whether I receive these privacy policies	1%	1%	0%
I have not received any such policies	2%	1%	0%

Education was also inversely proportional to privacy policy review, with 59% of those with no college degree reviewing health-related privacy policies, compared to 48% of respondents who had a college or graduate degree.

[10] This finding was also seen in the number of people that had not read the privacy policies, with only 11% of lower income respondents reporting that they did not read these privacy policies, compared to 8% of middle income respondents, and 22% of upper income respondents.

Table 27.

Education

	No College Degree	College Degree or Graduate Degree
Yes	59%	48%
No	12%	12%
Some of them	27%	38%
I am unaware whether I receive these privacy policies	1%	1%
I have not received any such policies	1%	1%

Age was predictive of whether individuals read health privacy policies, with only 37% of respondents in the under 18-25 demographic reading them, 52% in the 26-45 age-range reading them, and 56% of the 46-65 age-range reading these privacy policies.

Table 28.

Age

	Under 18-25	26-45	46-65	66+
Yes	37%	52%	56%	48%
No	14%	11%	12%	12%
Some of them	47%	35%	31%	33%
I am unaware whether I receive these privacy policies	2%	1%	0%	3%
I have not received any such policies	0%	1%	1%	5%

M. Health Privacy Policies--Conclusions.

We again see further evidence that income and education level is inversely related to health privacy policy review, and see here, in contrast to financial privacy, that age is a factor that must be considered. Once again, we see that the 46-65 cohort has the highest reported level of privacy policy review.

N. Cable Company Privacy Policies.

Overall, the review of privacy policies from cable companies was lower than those of other areas. 25% of respondents had reviewed the privacy policies they received from cable providers, 35% did not, and 31% reviewed some of them. This conclusion was consistent with the findings when respondents were asked to self-assess their sensitivity regarding information regarding their television viewing habits, because this data element ranked 99 out of 100 data elements based upon consumer perception of sensitivity.

Table 29.

	Total
Yes	25%
No	35%
Some of them	31%
I am unaware whether I receive these privacy policies	3%
I have not received any such policies	5%

Again, income and education level were inversely proportional to whether people reviewed these policies. 29% of lower income respondents reviewed these privacy policies, as did 28% of middle income respondents, compared to just 12% of upper income respondents, and 32% of lower and middle income respondents did not review these policies, compared to 52% of upper income respondents.

Table 30.

Income

	Lower	Middle	Upper
Yes	29%	28%	12%
No	32%	32%	52%
Some of them	30%	34%	30%
I am unaware whether I receive these privacy policies	3%	4%	3%
I have not received any such policies	6%	3%	3%

Consistent with other reported privacy policy review, 37% of those with no college degree reviewed these policies, compared to 19% of individuals with a college or graduate degree, and 26% of those with no college degree did not review the policies, compared to 40% of those with a college or graduate degree.

Table 31.

Education

	No College Degree	College Degree or Graduate Degree
Yes	37%	19%
No	26%	40%
Some of them	27%	34%
I am unaware whether I receive these privacy policies	3%	3%
I have not received any such policies	6%	4%

O. Cable Company Privacy Policies—Conclusion.

Once again, income and education levels were inversely proportional to privacy policy review, though age did not have an impact on this question.

P. Internet Service Provider Privacy Policy Review.

Generally, respondents reviewed ISP privacy policies at a lower level than other privacy policies, with 32% reviewing them, 35% reporting they had not reviewed the privacy policies, and 27% reporting that they had reviewed some of them.

Table 32.

	Total
Yes	32%
No	35%
Some of them	27%
I am unaware whether I receive these privacy policies	3%
I have not received any such policies	3%

Again, income level was inversely predictive of whether privacy policies were reviewed, with 32% of lower income respondents reviewing them, 37% of middle income respondents revering them, and only 23% of upper income respondents reviewing them.

Table 33.

Income

	Lower	Middle	Upper
Yes	32%	37%	23%
No	34%	29%	48%
Some of them	27%	28%	26%
I am unaware whether I receive these privacy policies	4%	3%	1%
I have not received any such policies	3%	3%	1%

A similar effect was seen when one considers the negative response to this question, with 34% of lower income respondents not reviewing these policies, 29% of middle income respondents not reviewing them, and 48% of upper income respondents not reviewing them.

Education level was similarly inversely predictive of privacy policy review, with 44% of respondents with no college degree reviewing these policies and 27% of this group not reviewing the policies, compared to 26% of respondents with a college or graduate degree who reviewed the policies and 39% who did not review them.

Table 34.

Education

	No College Degree	College Degree or Graduate Degree
Yes	44%	26%
No	27%	39%
Some of them	24%	29%
I am unaware whether I receive these privacy policies	3%	3%
I have not received any such policies	2%	3%

In this case, age was predictive of whether these policies were reviewed. 27% of those in the under 18-25 demographic reviewed these policies, 49% did not review them, and 18% reviewed some of them, compared to much higher levels at older age ranges, including the 46-65 demographic again being the highest rate of review.

Table 35.

Age

	Under 18-25	26-45	46-65	66+
Yes	27%	27%	38%	33%
No	49%	32%	32%	38%
Some of them	18%	35%	25%	25%
I am unaware whether I receive these privacy policies	4%	3%	3%	3%
I have not received any such policies	2%	3%	2%	3%

Q. Internet Service Providers—Conclusion.

The findings regarding ISP privacy policy review were consistent with the other data—education and income were inversely proportional to privacy policy review, and the 46-65 cohort had the highest rate of policy review.

R. Do People Read Other Documents?

Respondents were also asked whether they had reviewed other common documents, such as credit card agreements, leases or purchase contracts for automobiles, website terms and conditions, and their homeowners insurance policy. The results for these agreements appear below in the tables. It is important to note that certain privacy policies are reviewed at a similar level to important consumer contracts, but other privacy policies are not, which tends to support a conclusion that consumers are making active choices about which policies they want to spend time reading.

Table 36.

Have you read your homeowners insurance policy?

	Total
Yes	55%
No	18%
I don’t have one	27%

Table 37.

Websites—Do you read the terms and conditions for websites you visit?

	Total
Yes	54%
No	46%

Table 38.

Have you read the agreement (lease or contract) you entered when you purchased or leased your most recent car?

	Total
Yes	66%
No	34%

Table 39.

Have you read the agreement for any credit cards you have?

	Total
Yes	58%
No	21%
I do not have credit cards	21%

This data presents some interesting benchmarks for assessing the relative review of privacy policies. When review of certain agreements is compared as a matter of percentages, a relative ranking of document review can be created.

Table 40.

Have you read the agreement (lease or contract) you entered when you purchased or leased your most recent car?	66%
Have you read the agreement for any credit cards you have?	58%
Do you read the terms and conditions for websites you visit	54%
Health Care Privacy Policy Review	52%
Review of Financial Privacy Policies	44%
Internet Service Provider Privacy Policy Review	32%
Cable Company Privacy Policies	25%

One challenge with the data is that it is based upon respondents' self-reporting of conduct, and not a measurement of the conduct itself, and thus these results could be higher than if we measured actual conduct. One could conclude that the overall self-reporting bias, if any, was consistent across the categories, and therefore this table permits us to assess the relative review of all of these very common consumer-facing agreements and policies. Two conclusions can be drawn based upon this data, even assuming some self-reporting bias. First, with certain exceptions, privacy policies are generally reviewed as often as some very standard agreements—credit card and insurance agreements—that are routinely enforced. In other words, not everyone may review privacy policies, but they generally review them almost as often as some routinely enforced agreements in our society.

Second, consumers are making clear choices about their policy review, which seem at least in part based upon their level of concern about the data at issue. Television viewing history was the second least sensitive data element, and the finding that people reviewed cable company privacy policies less than other privacy policies is consistent with a conclusion that consumers are less concerned about this type of data, and thus choosing not to review these policies as often as they review other policies.

VI. Conclusions.

When respondents' self-reported sensitivity, as well as privacy protective behaviors are examined, some clear patterns emerge. Age is one of the most relevant factors to predict both privacy sensitivity, as well as privacy protective behavior, but it is not a linear relationship, and the 46-65 age range is consistently the most privacy sensitive and protective group. Education levels were, where relevant to sensitivity, inversely related, and clearly inversely related to privacy protective behavior. Income overall was not that significant in predicting sensitivity, but had relevance to predicting privacy protective behavior in the sense that higher income individuals were generally less likely to read privacy policies. Consumers also appear to be making choices about what agreements or policies they review, and it appears that the sensitivity of the information covered by the policy appears to influence the level of consumer review of these policies.

One main question to consider is how this information can help companies and consumers better understand privacy issues. It is a question that will require further analysis, but there are certain conclusions that are apparent. It seems clear from the data, particularly the data regarding privacy policy review and the inverse relationship between education level and policy review, that consumers are actively making choices about what privacy policies they review. While many may claim that "consumers do not read privacy policies", a categorical statement that does not appear to be accurate, a more accurate statement may be that consumers make active choices about what policies to review. It may be that consumers make value judgments about what they choose to spend their time reviewing, based upon their level of concern, but the general conclusions that consumers' refusal to read polices undercuts their effectiveness does not appear to be accurate.

A second conclusion is that companies can likely impact their brand in a positive way if they examine their customer base on a demographic basis and try and promote privacy in a positive way. As shown above, certain demographic segments are more concerned about certain forms of privacy, and this data can serve as the beginning of a roadmap to brand improvement on privacy.

A third conclusion is that consumers are likely not as careful as many would hope regarding their own privacy practices, particularly regarding carrying their Social Security cards and the failure to shred PII. While this does not directly correlate to companies' obligations, that data may be relevant in assessing businesses risk judgments regarding data disclosure and data destruction.

Fourth, and finally, whether a company is choosing to implement an information governance program, or PbD, this research represents the beginning of a roadmap for both types of programs. It is not the complete picture, and more research will be released by the Lares Institute regarding these issues, but consumers' attitudes and patterns regarding privacy protective behavior offer important insights as companies attempt to design privacy into their products and services, or implement governance regimes that implement best practices.

The Lares Institute

Data Breaches and the Phantom Damage Allegation

July 2011

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Lares Institute is pleased to present the results of *Data Breaches and the Phantom Damage Allegation*. There are a number of different reasons for companies to take data security and privacy seriously, which include: regulatory enforcement; brand damage; loss of market capitalization; and many others. Indeed, the recent, privacy-related allegations against a long-standing British newspaper, which effectively put the newspaper out of business, show the serious implications of a privacy mishap. Moreover, identity theft is a problem that presents a number of different potential issues for individuals and companies, and it can include the creation of new credit accounts, issues with medical records in the case of medical identity theft, misuse of existing credit accounts, and others.

However, when data breach cases are litigated, there are questions raised as to whether the information that was breached was actually used for identity theft, and as a result, plaintiffs typically raise claims that they are subject to increased risk of identity theft, though they have not suffered economic harm. A case arising from a retailer's alleged data breach presents a typical view of courts:

> Therefore, because the specific factual allegations of the Amended Complaint do not allege that the Plaintiff has personally experienced any injury other than 'hav[ing] been subjected to a substantial increased risk of identity theft or other related financial crimes,' the Court must accept the specific allegations Plaintiff makes as a true representation of the injury that the Plaintiff has suffered.[1]

Courts almost unanimously reject plaintiffs' attempts to plead damages because the plaintiffs are unable to present specific evidence of losses or damage, and this can be expressed by courts as a lack of "standing" to bring a claim, a plaintiff's inability to prove causation, or damages. The goal of this study was to help determine whether the courts are coming to the proper conclusion by asking survey participants if they could trace any unreimbursed losses back to a data breach. 30 percent of the participants responded that they had received a data breach notification in the last twelve months, 2 percent claimed they had suffered identity theft which they could not trace back to a specific security breach, and only 1 percent responded that they were able to trace losses to a specific data breach.

Furthermore, participants were asked to state how they were able to trace their losses to a specific breach. The responses call into question whether the 1.4 percent of participants who claim they could trace the losses back to a specific data breach could, in fact, trace the losses. This study supports the decisions made by courts in rejecting data breach claims, because plaintiffs cannot show loss resulting from a data breach.

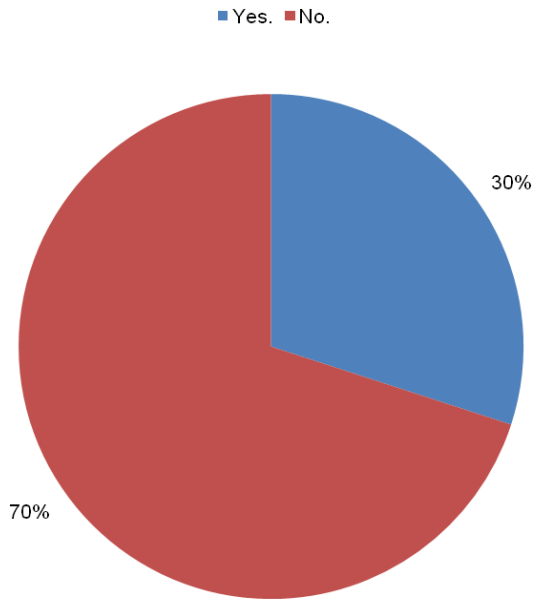
[1] *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 688–69, 66 Fed. R. Serv. 3d 447 (S.D. Ohio 2006) citing *Courtney v. Smith*, 297 F.3d 455, 459, 2002 FED App. 0248P (6th Cir.2002).

II. KEY FINDINGS OF THE SURVEY

The survey focused on data breach notifications received by the survey participants, and whether they had any unreimbursed losses that were attributable to a security breach. The following section presents the findings of the survey.

Survey participants were asked whether they had received notice of a security breach within the last twelve months. 30 percent responded that they had, and 70 percent responded that they had not.

Chart 1:
Q. Have you received notice of a security breach in the last 12 months?



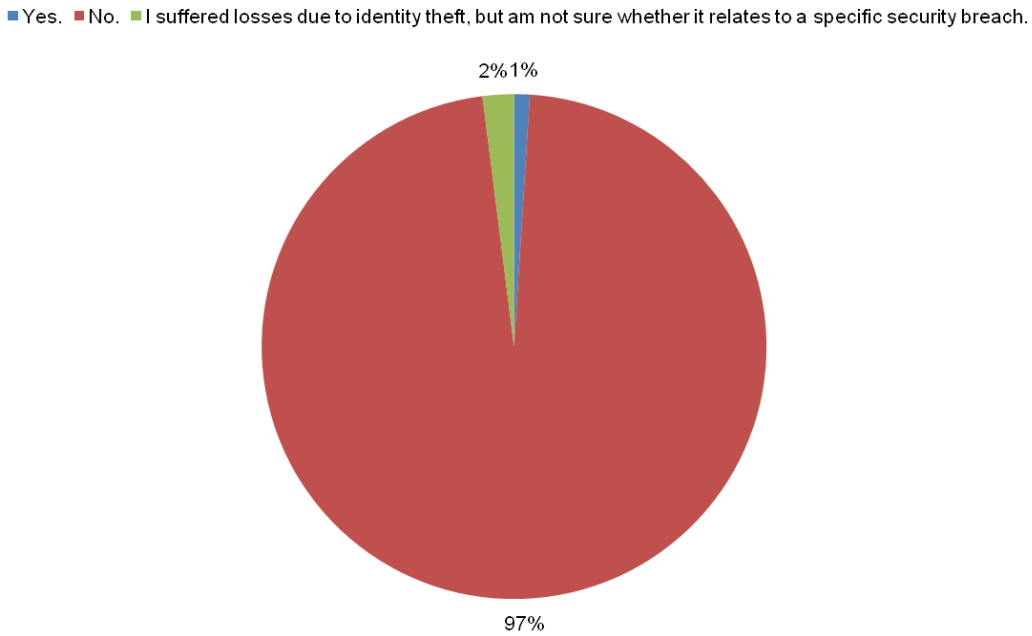
Of those who had received notice, 94 percent received between one and five, 2.7 percent received between six and ten, 2.7 percent received between eleven and thirty, 0 percent received between thirty and fifty, and less than 1 percent responded that they received more than fifty.

Chart 2:
Q. If so, how many notices have you received in the last 12 months?

Number of Notices Received in the Last 12 Months	
Answer Options	**Response Percent**
1-5.	94.0%
6-10.	2.7%
11-30.	2.7%
31-50	0.0%
More than 50.	0.7%

Survey participants were then asked if they had any unreimbursed losses that they could trace to a security breach that occurred in the last twelve months. 97 percent responded that there were none, while 2 percent suffered losses due to identity theft, but were not sure if it related to a specific breach, and 1 percent said there were some losses that were traceable to a specific security breach.

Chart 3:
Q. Have you experience any unreimbursed losses that you could trace to a security breach that occurred in the last 12 months?



Survey participants were then told to state how they were able to trace their losses to a specific security breach. None of the answers were able to provide details tying a breach to a loss; at most they were only able to trace it back to the person who used the information, not to the actual breach, which included statements like “unknown text bill charges” and “A purchase in a state I do not (nor have ever) lived…”

III. SURVEY METHODS

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. The survey was sent to 474 individuals in the United States, and 420 responses were received, for an 88.6 percent response rate. 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 that 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.

IV. A SUMMARY OF THE APPLICABLE LEGAL STANDARDS

Plaintiffs in data breach litigation must prove that they have standing to bring a claim, as well as harm that is proximately caused by a defendant's conduct.[2] In dismissing a case for lack of standing, the Southern District of New York, stated:

> The Court concludes that Plaintiffs lack standing because their claims are future-oriented, hypothetical, and conjectural. There is no "case or controversy." And, as noted, several other courts have reached the same conclusion in factually similar cases, both where data have been lost and where data have been stolen. For example, in *Randolph,* where a laptop computer belonging to defendant's employee and containing the personal data of some 13,000 individuals was stolen from the employee's home, plaintiffs alleged that they had been "placed at a substantial risk of harm in the form of identity theft" and that they had "incurred and will incur actual damages in an attempt to prevent identity theft by purchasing services to monitor their credit information." The court in *Randolph* determined that plaintiffs had "failed to demonstrate an injury that is sufficiently 'concrete and particularized' and 'actual or imminent.' And, in *Giordano v. Wachovia Securities, LLC, supra,* where a report containing financial information about plaintiff and tens of thousands of other customers was lost in transit and plaintiff "only allege[d] a potential injury," plaintiff was found to lack

[2] See, Serwin, POISED ON THE PRECIPICE: A CRITICAL EXAMINATION OF PRIVACY LITIGATION, 25 Santa Clara Computer & High Tech. L.J. 883 (2009); Serwin, Information Security and Privacy: A Guide to Federal and State Law and Compliance, Chapter 34) (2nd. ed. West 2010).

> standing. (citing *Luis v. Dennis,* 752 F.2d 604, 608 (3d Cir.1984) ("the alleged injury is not of sufficient immediacy and reality to permit adjudication by a federal court")).[3]

The *Hammond*, court also examined whether, even assuming standing could be found to exist, whether a claim for proximately caused damages could be sustained.

> Even assuming, *arguendo,* that Plaintiffs could be said to have standing, Defendant's motion for summary judgment dismissing Plaintiffs' claims would be granted because Plaintiffs' alleged increased risk of identity theft is insufficient to support Plaintiffs' substantive claims. ("Courts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy. Plaintiff has not presented any case law or statute, from any jurisdiction, indicating otherwise. Plaintiff's alleged injuries are solely the result of a perceived and speculative risk of future injury that may never occur. Plaintiff has failed to show an actual resulting injury that might support a claim for damages. As damages are an essential element of each of plaintiff's claims, plaintiff's claims fail as a matter of law.").[4]

V. CONCLUSION

The litigation process does not attempt, with very limited exceptions, to redress harms that have not yet occurred. As a result, as noted above, courts typically require plaintiffs to prove three distinct, but related elements to successfully bring a claim—standing, causation, and harm. Causation requires the person suing the company to show that the harm would not have occurred if it weren't for the actions of the company. Harm typically requires some form of economic damages, such as monetary loss (illegitimate charges on a credit card that are not reimbursed would fit in this category).

These requirements present often insurmountable hurdles for plaintiffs in data breach cases. Courts do not look favorably on claims based upon the possibility for future harm, and have been almost uniformly dismissing plaintiffs' attempts to recover in these cases. This study does not support a conclusion that companies should not have reasonable security practices, or that there are not risks that result from a lack of data security, and it should not be read to support a conclusion that data security isn't a core concern for all companies. It also does not focus on the cost to companies for data breaches, but instead focuses on whether plaintiffs in data breach cases suffer actual harm sufficient to state a claim for damages, and whether courts have accurately examined this issue. Based upon the results, it is clear that they have, because this study demonstrates that most individuals cannot prove any economic harm resulting from a data breach.

---

[3] *See*, *Hammond v. The Bank of New York Mellon Corp.*, 2010 WL 2643307 (June 25, 2010, S.D.N.Y.)(some internal citations omitted).

[4] *Id.* (internal citations omitted).

Chapter 39

A Reference For Your Company

§ 39:1 Introduction

As this book demonstrates, the number of laws that companies must comply with is staggering. This chapter attempts to identify common issues for businesses generally, as well as some industry specific issues. While comprehensive coverage of every issue is beyond the scope of this chapter, it does offer examples of pitfalls, as well as policies that companies should consider in order to highlight the most common and important issues. However, it does not catalogue every issue or law identified in the preceding chapters.

§ 39:2 General issues for companies—Marketing concerns

Common examples of general issues include Internet privacy and marketing concerns, commercial e-mail laws, TCPA compliance, including Do-Not-Fax concerns at the state and federal level. For many companies, e-mail and Internet-based marketing is a common form of branding and generating leads, so these issues are becoming all the more common. The CAN-SPAM checklist is a document that helpful for companies to understand their obligations, and companies must make sure they have adequate resources and policies to ensure compliance with the TCPA, including restrictions on auto-dialers or other similar devices. Also, policies that define the conduct of affiliates and other third-parties in the marketing context should be considered. Policies regarding the use of SMS for advertising is also a best practice because CAN-SPAM can also be implicated by the use of these type of wireless messaging.

Having an Internet privacy policy is also in many cases is required, and in most cases is a best practice even if not legally

required. While it is not a law that is commonly implicated, the Lanham Act can be implicated by statements made in a privacy policy, particularly if the issue is raised by a competitor. If applicable, ensuring that compliance with Internet-based privacy laws, such as COPPA, as well as other Internet-based statutes, such as the DMCA, is also important. Finally, having policies regarding the disclosure of identifying information, as well as IP addresses, is also important.

§ 39:3 Two party consent

One of the most challenging issues for companies is managing two-party consent issues.[1] While they are obvious in the telephone context, as evidenced by the disclosures that are made before calls are recorded or monitored, many of these same laws apply to electronic communications as well and can create issues when network, or email, monitoring is conducted.[2] This can be true even if the monitoring is done for security, or other reasons. These issues are generally discussed in Chapters 7 and 8, and particular attention should be paid to situations where real-time monitoring is done, where the communications also are made with non-employees, especially if the non-employee is a lawyer, or other person that can engage in a privileged communication. Discussion of when monitoring is considered to be real-time, versus a review of a stored communication, is contained in § 7:17.

§ 39:4 Defining the proper scope of investigations

The proper scope of investigations, including pretexting and wiretapping concerns, as well as concerns over disclosure of information in litigation are issues companies must address. Related issues regarding the permissible scope of searches of employees' offices, including their computers and personal e-mail accounts, as well as videotaping in the workplace are also frequent concerns as well. In some cases, the Fourth Amendment can be a concern in these situations if the government has asked a private citizen to gather information, or the employer is a government agency. There are also concerns over monitoring other forms of electronic communications, such as SMS and other similar forms of messaging, as well as concerns over reviewing communications that are potentially privileged, such as communications with an

---

[Section 39:3]

[1]See § 8:43.

[2]See, e.g., § 8:28.

employee's attorney or spouse. Restrictions on the use of polygraphs and concerns with the improper restriction of e-mail systems if union workers are present also are considerations for many companies. Moreover, the privacy implications of state constitutional and statutory rights of privacy are also important considerations.

Additionally, the implications of monitoring communications with third parties, including customers, are also a common concern, as is the monitoring of third-party web-based e-mail systems that are accessed with company resources. In certain cases The Patriot Act and FISA can also be implicated. Finally, managing employee background checks, including as part of the employment application process are also issues that companies must be aware of, as are managing issues regarding searches for employee information in publicly available arenas, such as the Web.

Policies that should be considered include policies regarding internal and third-party investigators, policies regarding the use of polygraphs, policies to define the proper scope of searches on company premises, as well as on company equipment, including computers. Having adequate disclosures and policies that inform employees that they do not have a reasonable expectation of privacy is also important, as are policies that define the acceptable use of employee background checks, as well as for compliance with the FACT Act rules on the use of medical information and the appropriate destruction of data should also be considered. Additionally, policies regarding responding to government investigations, including subpoenas are also important to consider.

§ 39:5 E-mail footers

A common question is whether an e-mail footer is required. Putting aside CAN-SPAM compliance (most companies place certain CAN-SPAM required information in the footer), there is no general requirement to have an e-mail footer. Certain industries typically place a disclaimer in the footer and many include a statement concerning the confidential nature of the e-mail and provide guidance in the case of unauthorized disclosure or misdirection. Other, in heavily regulated industries, include a statement regarding their monitoring policies.

§ 39:6 Defining "personally identifiable information"

While not an issue tied to any specific area of the law, defining what personally identifiable information is, including whether IP

addresses are personally identifiable, is a growing concern. As new forms of information become relevant to businesses and individuals, there will be growing concerns about these issues. The EU presents unique issues since there is some indication that the EU's view on IP addresses varies from the U.S. The framework identified by the Principle of Proportionality is important to utilize as a guide for these type of issues.

§ 39:7 Information security requirements

Information security is an issue all companies must face. While the amount of resources devoted to information security will vary given the sensitivity of the data, this issue, particularly in light of FTC enforcement actions and the number of state and federal laws identified herein, is one all companies must consider. Having a plan, including an incident response plan, is helpful and placing appropriate safeguards is also important. Restricting access to sensitive information is also a strategy companies should follow. Making sure all appropriate third parties are bound to meet applicable standards is also something that most companies must consider. Having a plan, including an incident response plan, is helpful and placing appropriate safeguards is also important. Restricting access to sensitive information is also a strategy companies should follow. Making sure all appropriate third parties are bound to meet applicable standards is also something that most companies must consider. Making sure that there is an appropriate level of auditing and compliance for your company is also important. Making sure all of the relevant software is updated and common vulnerabilities are addressed is also an important step.

The importance of these issues is reflected in laws such as SOX and other federal laws have either data security, or data destruction requirements. Obviously, the FTC Act and its restrictions on deceptive trade practices and unfair acts, as well as the accompanying guidance given by the matters brought by the FTC are important for any company to consider in the data security context since data security is a fertile ground for FTC activity. Recent FTC guidance discussed in this book on safeguarding information is also of import. Data security policies, including restrictions on third-parties are policies that should be considered and implemented by many companies.

Moreover, new state laws in Massachusetts and Nevada have raised additional concerns on the information security front, and determing the application of these laws to your business, as well as meeting the compliance burdens, if applicable, is something that must be considered by most companies.

§ 39:8 Insurance, indemnity and other risk shifting mechanisms

In many cases, assessing and appropriately allocating risk for information security and privacy incidents can result in significant savings for your company. There are now brokers who specialize in these types of insurance products and finding the appropriate policy can be very beneficial. Moreover, thought should be given to risk allocation in most contracts where personally identifiable or sensitive data is at issue. Thinking through whether there will be a cap on liability for data issues, who will pay for notice of a security breach, as well as credit insurance for the individuals, and even who will give notice in the event of a breach should be considered. Common issues with indemnities generally should be addressed, including issues regarding the scope and nature of any defense obligation if there is litigation, what level of fault by the indemnified party precludes indemnity, and issues regarding control of the defense and settlement of third party claims.

§ 39:9 Computer crime laws/Confidential information concerns

Computer crime laws are of import (the Computer Fraud and Abuse Act in particular), including for entities that have significant trade secrets since these laws can be triggered if employees take electronically-stored confidential information, or access systems that they are not permitted to. The related Economic Espionage Act is also a law that companies can use to protect their confidential information, as is state trade secret law. Policies that restrict employee access to only those with a need to know confidential information are important first steps, as are policy statements restricting access by competitors of websites that contain confidential or proprietary information. Data security policies regarding access to these types of information are also key for companies.

Computer crime laws are potentially implicated when subpoenas are issued to Internet Service Providers. There are also litigation issues that must be addressed and considered when subpoenas are issued for these types of information.

§ 39:10 Anonymous subpoenas

Anonymous subpoena issues are also important to many companies as they may face a situation where they need to identify an anonymous speaker on the Internet, or in e-mail, who

seeks to do the company, or its employees, harm. While specific policies are not necessarily required, addressing this issue as part of an overall incident response plan can be helpful for companies that face these issues.

§ 39:11 Blogging and social networking

The use of blogs and social networking sites, particularly as part of a company's communication strategy, raise a number of issues, and implicate many laws discussed in this book, including cyberdefamation, disclosure of confidential information, marketing laws, as well as liability for statements by employees to other employees, or third parties. Policies regarding the appropriate use of these types of communication vehicles, particularly if they are in some way sponsored by the company are good steps to try and limit liability and exposure of inappropriate information. If these resources are not officially part of a company's communication strategy, or otherwise officially sanctioned, raise issues of misuse of company networks and computer resources, in addition to those issues raised above, and companies should consider appropriate policies to restrict access to these type of services.

Moreover, as discussed in Chapter 33, the FTC has issued new guidance regarding the use of blogs regarding the promotion of products, which must be complied with.

§ 39:12 Security breaches

Security breach laws are top of mind for many companies these days, and the closely-related security freeze laws also may need to be complied with. Companies should take steps to try and reduce the amount of data they collect so that the chance of a security breach is reduced. Moreover, if truly sensitive data is at issue some forms of monitoring may assist companies in preventing, or limiting security breaches. As more fully discussed in Chapter 25, there are a number of differing requirements under the now 44 state (plus New York City, Puerto Rico, and Washington D.C.) security breach laws and care should be taken to comply with these laws. Having an incident response plan in place will assist your company with gathering evidence of the breach and providing timely notice to individuals, as well as other relevant entities. The plan should identify other necessary documents that need to be prepared in case of a breach (such as FAQs), identify key personnel that need to be notified, including executives and other managing agents, as well as internal or external P.R. resources, if appropriate. Key members of IT, including any necessary outside forensic consultants, should also be identified.

§ 39:13 Security freeze laws

Security freeze laws permit a consumer to place a "freeze" on their consumer reports. While this places a number of burdens on the consumer reporting agencies, it also places obligations and restrictions on other businesses that obtain or use data from consumer reports. Policies to assist your business with these laws, even if you company is not a consumer reporting agencies, are a good idea that can greatly assist your company.

§ 39:14 Red flag regulations

While not effective as of the date of this book, the "red flag" regulations promulgated under the FACT Act also are notable for businesses because they effectively apply to any company that extends credit, and require monitoring of certain activity that can indicate identity theft as well as steps to reduce identity theft. Policies to implement these requirements are mandated by these regulations so businesses must address these issues sooner rather than later.[1]

§ 39:15 Electronic Health Records

A new focus on EHR and the privacy and security concerns that are raised is the result of the HITECH Act, which was part of the ARRA passed last year. As with HIPAA, while privacy and security are not the focus of laws implementing EHR, the privacy and security concerns and regulations created to protect privacy and security are key to the implementation of EHR.

§ 39:16 Social Security numbers

Restrictions on the use and disclosure of Social Security numbers are also important to most companies. There are a number of states that prohibit the posting, display, or transmission in certain circumstances, of Social Security numbers, unless otherwise permitted or required by law. This is an important issue for many companies because Social Security numbers are

---

[Section 39:14]

[1]At the request of several members of Congress, the FTC further extended the enforcement deadline for the Identity Theft "Red Flags" Rule, through December 31, 2010. This extension will allow Congress to consider legislation that would affect the scope of entities covered by the Rule. The announcement of the extension and the release of an Enforcement Policy Statement do not affect other federal agencies' enforcement of the original November 1, 2008 deadline for institutions subject to their oversight to be in compliance.

often a critical piece of identifying information. However, they are also frequently the target of identity thieves. As such, companies should consider implementing policies that limit the use, collection, display, or transmission of Social Security numbers.

§ 39:17 Credit card receipt issues

The FACT Act's restrictions on the printing, and likely computer display, of credit card numbers on receipts (including the more restrictive state laws) also impact many companies. In 2009, new, more restrictive requirements went into effect in California, which include restrictions on the storage of credit card receipts with numbers on them, so while dedicated policies may not ultimately be necessary, actively monitoring for compliance is critical because there have been a number of lawsuits brought for the violation of these laws.

§ 39:18 Spyware, phishing and pharming

Many businesses suffer from issues related to spyware, phishing and pharming attacks. Businesses are sometimes targets of spyware attacks that seek to obtain personal information or other confidential information. Moreover, many companies have their logos or web code used improperly as part of phishing or pharming attacks. Policies related to intellectual property enforcement, particularly trademarks, can be implicated and prove helpful in phishing and pharming situations, and all of these issues, including spyware, can implicate a company's data security policy.

§ 39:19 Cloud computing

Cloud computing is a recently developed style of computing that uses the Internet to provide programs and resources. Because the resources are shared on the Internet, there are a number of privacy and data security concerns, as well as concerns over data ownership and control. While there are no laws that specifically address cloud computing, privacy and security laws discussed in this book are applicable and it is likely that new laws will be passed to cover this emerging area.

§ 39:20 Transfers in M&A, bankruptcy, and retroactive changes to privacy policies

In the merger and acquisition context, as well as when there is a potential bankruptcy of a company, making sure that transfers of information is permitted is something which companies must

be cognizant. Having a privacy policy that contemplates these issues can be critical, particularly if the change is to be applied retroactively.

§ 39:21 Internet concerns

Doing business on the web opens a company up to a variety of issues that must be addressed. In addition to the issues identified previously regarding marketing, making sure your company does not collect more information than it needs via the web, as well as ensuring that any transfers of sensitive personal information are handled securely, are important. Moreover, concerns over the collection of date of birth are issues that companies must address even if they are not sites targeted to children 12 and under because merely collecting a data of birth can potentially make the company have to comply with certain portions of COPPA.

While not purely a privacy issue, the Communications Decency Act can impact businesses both from blocking their ability to sue the "publisher" of a defamatory publication on the Internet, as well as potentially protecting them from liability for certain postings on their Internet pages. This is all the more true under the new guidance from the Ninth Circuit, discussed in Chapter 4.

Finally, the DMCA also can have privacy implications because content owners can request the disclosure of certain personally identifiable information to identify alleged infringers and companies should consider having policies in place to deal with these type of requests, as well as the removal of content if it is infringing, the limitation or elimination of access to the website or service for repeat offenders, and counter-designation policies for people who are accused of infringement and dispute the allegations.

§ 39:22 Public display of information

A number of states have restricted certain entities from publicly displaying personally identifiable information regarding law enforcement and other individuals, particularly if there is a threat of harm. These issues are generally discussed in Chapter 2, and an overview of the issue is included in § 2:34.

§ 39:23 Behavioral advertising

While the issue has recently come to light again, and will continue to grow in importance, behavioral, or targeted, advertising, is an issue that has broad implications for many companies. This type of advertising uses data about the consumer that is

gathered by the company, or a third party, to target certain advertisements to the consumer. This is an area where the FTC is actively engaged and is attempting to set best practices. Typically concerns center around notice and choice for consumers regarding their information. Setting standards and considering the type of linkage between advertisements and personally identifiable information, as well as limiting the broad dissemination of this type of information is something that companies must consider.

Internet companies that have a search engine function also have unique issues regarding the retention, processing, and disclosure at government request, of search engine data which in many cases is retained and used as part of behavioral advertising.

§ 39:24 Genetic privacy

With the arrival of GINA, genetic privacy has now arrived as a top of mind issue. While GINA has federalized a common standard, there are a number of state laws that are also relevant. Typically, these laws prohibit discrimination by employers or insurers based upon genetic information. There are also restrictions on the use of genetic testing of individuals, as well as their family members in certain cases. Civil remedies are typically available for the breach of these laws.

§ 39:25 Payment Card Industry standards

For any company that permits customers to use credit cards, PCI standards, which are set by the credit card companies, are a growing area of concern and the recent laws that have been enacted in certain states that impose liability on merchants that improperly retain certain credit card information is also a compliance hurdle. The PCI standards are quite detailed and compliance is mandatory in most cases. Having the requisite policies in place is critical because failures in this regard can lead to identity theft, as well as the loss of the ability of the merchant to accept payment by credit card.

§ 39:26 Biometrics

The gathering and processing of biometric data is an issue that is becoming more of a concern. Many companies are starting to consider using biometric data as an identifier and one of the major drawback is that once it is compromised it cannot be changed. As a result, there have been some concerns about its use, as well as civil liberty issues raised over the use and processing of

fingerprints. While specific policies are not necessarily required, they should be considered and the reduction or elimination of the collection of unnecessary biometric data should be considered. In certain cases, a numerical representation of the biometric data can be collected, which may reduce some of these issues.

§ 39:27 RFID/GPS

Radio Frequency Identification is a growing concern, as is the use of GPS systems. RFID and GPS can be used to track goods, as well as individuals, in certain cases. Cell phones all have GPS tracking built-in that can be monitored by the government in certain cases. Moreover, certain states require parolees to be monitored via GPS. This type of technology raises civil liberty concerns, particularly as the ability to track individuals is increasing, but it offers a significant advantage to business in that it permits increased monitoring and control of goods.

§ 39:28 International issues

As businesses become more global, concerns over the international transfer of information, particularly to the United States, are increasing and international privacy is a large compliance issue. Whether it is customer data, or data regarding your company's employees, many countries impose significant restrictions on the transfer and processing of data in the United States. Moreover, as noted in *Information Security and Privacy: A Guide to International Law and Compliance*, there are many conflicts with United States and international law, including with SOX, so managing compliance can be challenging. Moreover, when systems are implemented to share contact and other information regarding employees across borders, there can be significant risk and compliance issues. As discussed in *Information Security and Privacy: A Guide to International Law and Compliance*, many companies are starting to opt to comply with the EU laws via Binding Corporate Rules, although Model Contracts and Safe Harbor also remain as available options. BCRs require extensive policies, as do the other two options for EU compliance, so care must be taken to ensure that all necessary policies and training are implemented.

Moreover, differences about the definition of what is personally identifiable information, particularly the brewing debate over whether IP Addresses are personally identifiable in the EU, is also an issue that companies must address.

§ 39:29 SOX

For publicly-traded companies, the internal controls require-

ments of Sarbanes-Oxley, as well as Rule 404, are privacy and data security concerns. If there is no data security regarding the company's sensitive data, particularly financial data, in many cases the company may lack internal controls. As noted above, whistleblower requirements can conflict with EU laws, so finding the correct compliance path can be challenging.

§ 39:30 Responding to government requests

Compliance with the Patriot Act, as well as the Foreign Intelligence Surveillance Act, including responding to National Security Letters, is a less common, though important issue. Having the appropriate policies in place to ensure compliance with these requests is critical for companies, particularly those, such as telecom companies and ISPs, that receive a number of these type of requests.

§ 39:31 Application of consumer reporting agency laws

One issue that has received some legislative attention is regulation of consumer reports. These laws are typically use-based restrictions and the laws typically only apply to certain types of entities—consumer reporting agencies. While there are 3 clearly recognized consumer reporting agencies that maintain files on a nationwide basis regarding consumers, many of these laws, particularly at the state level, sweep many other companies into their definition of a consumer reporting agency. As a result, companies other than the "Big 3" need to consider whether they are regulated by these laws. A selection of these laws is discussed in Chapter 17.

§ 39:32 Employment applications

While the Fair Credit Reporting Act, and the state analogues, are focused on financial issues, many other forms of conduct are regulated by these laws, including employers' use of information in connection with hiring, or firing employees. These laws are discussed in Chapters 16 and 17.

§ 39:33 Industry specific concerns—Energy companies

Energy companies face some unique privacy and security issues. In many cases there are additional privacy burdens imposed on utilities in state Public Utility Codes. There are also restrictions regarding the denial of credit to victims of identity theft in certain circumstances. Moreover, given the unique physical security issues that many companies face given this central

nature of this industry to the American economy, there is a different level of balancing of privacy interests that may result in more extensive security clearance and background checks, as well as restrictions on offshoring certain data. In addition to increased physical security, in many cases increased technical and administrative security are also common, particularly if there are nuclear plants involved. Also, the Red Flag regulations are important to note as well.

§ 39:34 Industry specific concerns—Financial institutions

Financial institutions are subject to a number of special requirements under state and federal law, including GLB, FCRA, and state financial privacy laws, as well as lending laws that can have privacy and information security implications. A complete discussion of these additional requirements, including the requisite policies, is contained in the relevant chapters, but common issues include concerns over affiliate sharing, making sure all required notices under these statutes, particularly GLB, are given, and information security. Pretexting is also a concern for financial institutions and it is specifically regulated under GLB, as is compliance with the Bank Secrecy Act.

§ 39:35 Industry specific concerns—Hospitals and medical providers

HIPAA is one of the more well known privacy laws, though it was not truly intended as a privacy law. Covered entities must comply with HIPAA, as well as more restrictive state law in certain cases, regarding the disclosure of PHI, or Protected Health Information. Privacy and security policies are required to comply with HIPAA, as are audits, assessments, training, and other requirements. Health care providers also must comply with infectious disease laws, which in some cases prohibit, mandate or permit disclosures, as well as restrictions on the storage, retention, and destruction of medical records. Moreover, entities that are not covered by HIPAA, as well as those that are, are also subject to medical marketing laws, and certain states have enacted restrictions on the disclosure of physician's prescription history.

Genetic privacy, including how information used for research regarding the human genome can be processed, are also concerns for health care, and related, entities.

§ 39:36 Industry specific concerns—Government employers

Government employers face unique disclosure and privacy

issues. In many cases, government employers are subject to FOIA, or similar public records requests, so they may be under broad disclosure obligations. However, they are also subject in many cases to Fourth Amendment warrant requirements before they search an employee's computer, depending on the circumstances of the search and seizure. There are also restrictions upon the posting of certain information regarding government employees by others that are important to note.

§ 39:37 Industry specific concerns—Social Networking sites

Social networking sites are at the forefront of many privacy issues. They face many issues that all companies face, but must address them in unique ways, because the very purpose of the service is to share personal information, including information that can be very sensitive. Concerns over the DMCA, the CDA, behavioral advertising, government requests for information, as well as many other issues must be addressed. Balancing the need for disclosure on the sites, with user's privacy expectations, is often the most difficult issue to address.

§ 39:38 Industry specific concerns—The airline industry

Given the unique physical security issues faced by the airline industry, there are unique privacy concerns, and a different balancing of expectations of privacy. Airlines are much freer to search individual's personal belongings, and airports obviously serve in many cases as the site of a border search, though this is not done by the airlines themselves. Disclosures under FISA and the Patriot Act are common concerns, as is the related and ongoing debate with the EU over the disclosure of Passenger Name Records, or PNRs.

§ 39:39 Industry specific concerns—Retail issues

Retailers face a number of privacy issues, which in part arise from their collection of information consumer buying patterns, as well as collection of payment information. PCI compliance and other issues regarding credit card information (including credit card receipt laws) are common concerns, but these are just the beginning. Data destruction is a common issue, and behavioral advertising is becoming a larger issue for retailers, as shown by the recent FTC enforcement action against Sears. The Red Flags Rule also can impact retailers and many other laws can raise compliance hurdles.

§ 39:40 Industry specific concerns—Telecom

Telecom companies face a number of issues, both as ISPs, as well as telephone providers. Pretexting, NSLs, Patriot Act compliance, as well as disclosure to the government of other information, including under the ECPA and Pen Register laws are also common concerns. Subpoenas in civil litigation that seek to identify users who have engaged in misconduct are also common issues that must be addressed by telecom companies, including under the DMCA. There are also Public Utilities Code restrictions on telecom providers regarding the disclosure of certain forms of information. Cellular providers face similar issues in different contexts, including the disclosure of SMS content, but they are subject to some different requirements.

§ 39:41 Industry specific concerns—Insurance companies

Insurance companies must comply with many of the financial privacy laws, to the extent they are covered by them, but they must also comply with state insurance privacy laws. They also face issues similar to those faced by financial institutions regarding security of information under many of these laws, or the general information security laws, given the sensitivity of this information. Medical privacy laws can be implicated in certain circumstances, depending upon the nature of the information contained in the insured's file, as well as the source of the information.

§ 39:42 Industry specific concerns—Publishers

Publishers, particularly those on the Internet, frequently face issues about the disclosure of anonymous posters, as well as First Amendment concerns over the reporter's right to keep the identity of their sources private. The publisher may in many cases set a policy to determine if, or when, it will disclose these types of information.

§ 39:43 Industry specific concerns—Cable and video companies

Cable and video companies are subject to particular privacy requirements that prohibit the disclosure of subscriber information. As DVRs become more common, questions regarding the disclosure of information gathered from these devices will be raised, including whether this information is covered under existing law. A related issue is what standards apply to cable providers when they are providing ISP services, and are not simply

providing cable service only and there is a conflict in the law on this point. Cable companies and video companies face a number of issues that are similar to telecom companies, including managing government requests for information.

