North Carolina State University Computer Science Technical Report # TR-2009-16
Submitted to IEEE Security & Privacy (July 29, 2009)

How Internet Users' Privacy Concerns Have Evolved Since 2002

Annie I. Antón[1], Julia B. Earp[2], Jessica D. Young[1]

[1]College of Engineering, North Carolina State University, Raleigh, NC 27695-8206, USA (919.515.5764)
[2]College of Management, North Carolina State University, Raleigh, NC 27695-7229, USA (919.513.1707)

{aianton, julia_earp, jdyoung2}@ncsu.edu

Abstract

In 2002, we established a baseline for Internet users' online privacy values. Through a survey we found that information transfer, notice/awareness, and information storage were the top online privacy concerns of Internet users. Since this survey there have been many privacy-related events, including changes in online trends and the creation of laws, prompting us to rerun the survey in 2008 to examine how these events may have affected Internet users' online privacy concerns. In this paper, we discuss the 2008 survey, which revealed that U.S. Internet users top three privacy concerns have not changed since 2002; however, their level of concern within these categories may have been influenced by these privacy-related events. In addition, we examine differences in privacy concerns between U.S. and international respondents.

1. Introduction

In 2002, we created and validated a survey instrument to establish a baseline of Internet users' privacy concerns [EAA05]. The instrument was developed using a subset of the Antón and Earp privacy goal taxonomy [AE04] as a theoretical foundation. The taxonomy categories were used to express dimensions of privacy concerns and included the following: access/participation, information collection, information storage, information transfer, notice/awareness, and personalization. The 2002 survey revealed that Internet users are primarily concerned about information transfer, notice/awareness, and information storage. Another primary finding of that study is that Internet users' privacy concerns and online privacy policies are misaligned because privacy policies at that time primarily emphasized data integrity/security, information collection, and user choice/consent. Thus, there was no overlap between the top three privacy concerns among Internet users and the items that were most emphasized in Internet privacy policies. In 2008, we repeated the survey. This paper explores how Internet users' privacy concerns have evolved between 2002 and 2008.

Many privacy-related events have occurred since 2002, prompting us to rerun our survey, using our validated survey instrument, to examine whether and how individuals' privacy concerns have evolved. In addition, this entails considering how the environment has evolved in terms of changes and trends in online shopping, introduction of new laws, etc. For example, the Health Insurance Portability and Accountability Act (HIPAA)[1] was enacted in 1996, but compliance was not required until 2003. Therefore the compliance date occurred after the first survey and before the second. People may be more aware of privacy notices today than in 2002 for a variety of reasons. For example, consider that after the 2003 HIPAA compliance date, anyone who visited a healthcare facility started receiving privacy notices and were required to sign a statement indicating that they had received and/or read that organization's privacy notice.

The economic and legal landscape also changed over the course of the six years between our first and second surveys. Consider, the U.S. Census Bureau's data[2] that shows an increase in U.S. e-commerce retail sales from 10.2 billion dollars during the second quarter of 2002 to 31.6 billion dollars during the third quarter of 2008. Clearly, there has been a significant increase in online shopping since 2002,

[1] Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[2] http://www.census.gov/mrts/www/ecomm.html

suggesting that Internet users may be more comfortable in sharing their sensitive financial information, such as credit card numbers, with websites.

In addition to the increase in online shopping, there has also been an increase in online professional and social networking since 2002. Professional and social networking allows individuals to connect with co-workers, friends, family, classmates, and others online. LinkedIn,[3] a professional networking site, was founded in May 2003. By October 2008, it had 33 million users. MySpace, a social networking site, was founded in the fall of 2003[4] and by January 2008 it had 110 million active members.[5] Another social networking site, Facebook,[6] was launched in February 2004. By the start of the second survey in August 2008, Facebook had over 100 million active users. These numbers show that people are increasingly putting varied information about themselves online.

Individuals appear more willing to speak out today about what they perceive as invasions to their privacy when engaging in online activities. For example, in February 2009, Facebook changed its Terms of Service regarding its information practices, resulting in public outcry from its members, which manifested in the creation of many Facebook user groups to protest the change. In response to this public outcry, Facebook reverted back to its previous Terms of Service as they began crafting their next version to reduce the problematic verbiage.[7]

Along with the increase in online shopping and professional/social networking, the number of consumer complaints about information practices has also increased. The U.S. Federal Trade Commission's (FTC) Consumer Sentinel Network[8] has an online database of consumer complaints addressing, for example, fraud and identity theft. We examined the Consumer Sentinel Network Data Book,[9] a summary of this consumer complaint database. The Data Book contains statistics about the complaints, descriptions of the complaint categories, and sample complaints, as well as descriptions of Consumer Sentinel Network member organizations and how much information each contributes to the database. The total number of annual complaints has continually increased each year more than doubling since 2002. Individuals are submitting more complaints today, suggesting that people may be more aware and/or concerned about their sensitive information as it pertains to identity theft and fraud.

Reports of lost laptops or sensitive information leaks in the press are becoming more frequent. Consider the data loss events that are addressed in the press and chronicled by the Privacy Rights Clearinghouse's *A Chronology of Data Breaches*[10] using data from the Open Security Foundation's DataLossDB;[11] this appears to be the most comprehensive list of data loss events available. Within the database, only sixteen events were reported before the start of our first survey in 2002 with no events reported during the time the survey was running. In contrast, at the start of the second survey the database contained 1,370 reported events and 47 additional events occurred while the survey was running.

In response to concerns about the need to notify individuals' whose sensitive information has been compromised, states are passing data breach notification laws. Currently forty-four states and the District of Columbia have data breach notification laws. Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota are currently the only states without data breach notification laws. These laws, which vary by state, require companies to notify consumers when breaches involve their personal information. California was the first state to have a data breach notification law, which became effective on July 1,

[3] http://press.linkedin.com/history
[4] http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=120412
[5] http://www.web-strategist.com/blog/2008/01/09/social-network-stats-facebook-myspace-reunion-jan-2008/
[6] http://www.facebook.com/press/info.php?timeline
[7] http://blog.facebook.com/blog.php?post=54746167130
[8] http://www.ftc.gov/sentinel/
[9] Federal Trade Commission, "Consumer Sentinel Network Data Book for January – December 2008," February 2009, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf
[10] http://www.privacyrights.org/ar/ChronDataBreaches.htm accessed on April 20, 2009.
[11] http://datalossdb.org/ accessed on April 20, 2009.

2003. The next wave of data breach notification laws came two years later in 2005. Figure 1 chronologically plots reported data loss events as well as the effective dates for state-based data breach notification laws. We verified the effective dates for these laws in at least two sources and combined these dates with the data loss event dates from the previously mentioned DataLossDB. Within Figure 1, the blue diamonds represent individual data loss events and the red squares represent the effective date for the different state-based data breach notification laws. The gray vertical bar in 2002 marks the time during which we conducted our first survey, whereas the gray vertical bar in 2008 marks the time during which we conducted our second survey. Prior to the data breach notification laws, very few data breaches were required by law to be publicly reported. It is plausible that these new laws have led to the increase in publicly documented data breach incidents.

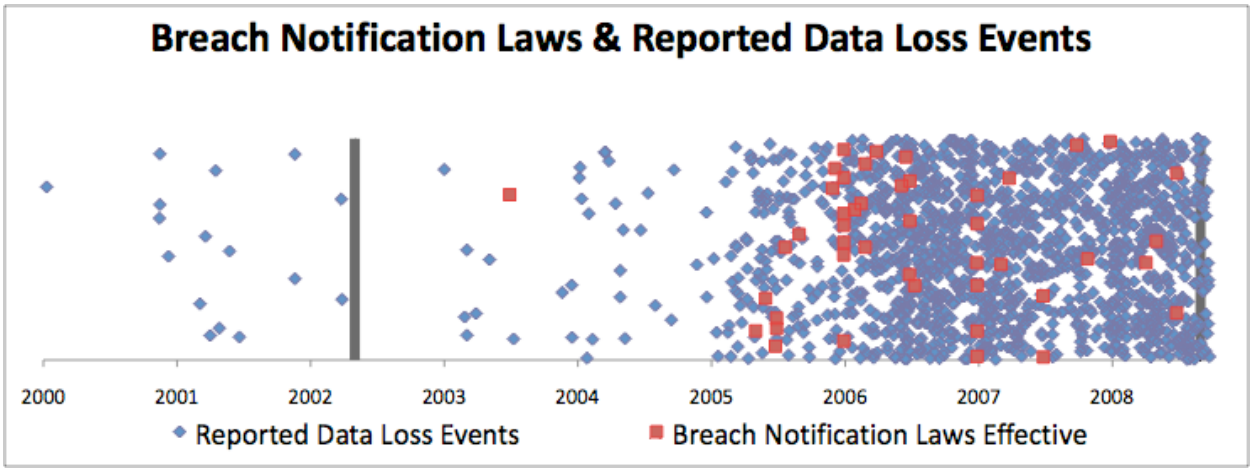

Figure 1: Breach Notification Laws and Reported Data Loss Events[12]

In addition to data breach laws, most states now have security freeze laws to protect consumers from identity theft. These laws allow consumers to put a hold on their credit files to avoid others from being able to fraudulently open new accounts using stolen information. The first security freeze law came into effect in California in 2003. Today, Washington, DC and 47 states (excluding Alabama, Michigan, and Missouri) have passed security freeze laws. These laws vary from state to state; for example, in Arkansas, Kansas, Mississippi, and South Dakota, the freeze only applies to identity theft victims who have filed a police report, whereas the other states allow any consumer to place a security freeze on his/her own account. In 2007, the credit bureaus began granting all consumers the ability to set security freezes on their accounts; if a given state law applies a lower fee than the credit bureaus' fees, the lower fee applies.[13]

2. Survey Methodology & Results

The survey conducted in 2008 is based on our prior research to create a validated survey instrument. The validated survey instrument enabled us to establish an Internet users' privacy values baseline. This section discusses why and how the survey instrument was developed, the results of the 2002 survey as well as the results of our 2008 survey.

2.1 Survey Instrument & 2002 U.S. Survey Results

In establishing our survey instrument, we sought to understand consumers' information privacy concerns [EAA05]. In addition, we employed the information obtained from our content analysis of healthcare privacy policies to further examine how individuals' online privacy concerns align with the

[12] This figure was generated from: http://datalossdb.org data accessed on April 20, 2009
[13] http://www.worldprivacyforum.org/creditfreeze.html

information expressed in privacy policies by organizations that are regulated by the HIPAA. The content analysis provided guidance for developing the survey instrument. The survey statements (see Appendix A) are grouped according to six dimensions of privacy concerns based on the following classifications—personalization, notice/awareness, information transfer, information collection, information storage, and access/participation [EAA05]. A comprehensive description of each category can be found in [AE04]. The survey ran from April 5, 2002 to May 31, 2002, and produced 1,005 usable responses with 827 of these responses representing individuals in the United States.

Our 2002 study revealed that the statements occurring in companies' privacy policies were not aligned with the survey respondents' information privacy concerns [EAA05]. Policy statements at that time primarily emphasized characteristics of the following dimensions from the Antón and Earp taxonomy: data integrity/security, information collection, and user choice/consent. In contrast, the U.S. respondents' primary concerns in rank order were: information transfer, notice/awareness, and information storage [EAA05]. This misalignment raised awareness for the need to better align corporate privacy policies with consumers' privacy concerns to ensure that individuals can make informed decisions about the companies to whom they entrust their information.

2.2 2008 U.S. Survey Results

Because the Internet has evolved so much since 2002, we employed our validated survey instrument again in 2008 to examine whether individuals' privacy concerns have changed as a result of the previously discussed external influences. The 2008 survey was available online from August 11, 2008 through September 29, 2008 and produced a total of 2,094 usable responses. Of these responses, 1,525 represent individuals in the U.S., 527 represent individuals outside the U.S., and 42 indicated "Rather not say" for the country of primary residence. The survey was advertised using a wide variety of dissemination mechanisms, including physically posting fliers on bulletin boards around campus; posting announcements on academic websites as well as professional and social networking sites; and sending emails to our own personal and family networks.

The 2008 survey resulted in a much larger sample size; therefore, we are not comparing two identical samples. However, the survey demographics for the 2008 survey are similar to those of the 2002 survey. In both surveys, the majority of respondents were male and the largest participant group was the 22-28 age group. The majority of the 2008 U.S. respondents have more than a college degree, or some graduate schooling. Although this does not parallel the average education level of Internet users over age 25 (14.4 years, or two years of college) [AEH04], we can still make important inferences from this study.

In the 2008 survey, respondents were required to respond to all items. Whereas the survey's demographic items provide a "Rather not say" option to respondents, the 2002 survey allowed respondents to omit these items, resulting in "No response" in some cases. The 2008 survey modified this option by not accepting missing responses. As with any survey, there are always concerns about whether participants are completely honest when responding. Several measures were taken to avoid incorporating dishonest users' responses into the participant dataset, including: requiring questionnaires to be completed before submission; ensuring the anonymity of participants be preserved; and removing responses from the dataset if they were deemed invalid.

Changes in Internet usage were revealed when comparing the 2002 and 2008 respondents. As compared to the 2002 survey, the latest survey showed that respondents use the Internet more now ($p<0.0001$)[14] with the majority of respondents spending more than 20 hours online a week. In 2002, 63.6% of the respondents made online purchases once a month or less. There is a statistically significant increase in the frequency of online purchases made by individuals in 2008, with 78.8% of respondents purchasing online more than once a month. Additionally, respondents are engaging in more online

[14] In this study, the p-value represents the probability that the observed difference occurred by chance. A low p-value ($p<0.05$) corresponds to a stronger result.

activities. Consider that in 2002, the only online activity in which over 40% of respondents were engaged in was product purchasing. In contrast, in 2008, education, financial services, product purchasing, and research were all activities for over 70% of the respondents.

Our 2008 survey revealed that individuals' information privacy concerns have not changed since 2002. The top three information privacy concerns continue to be information transfer, notice/awareness, and information storage. What has changed is individuals' level of concern as we now discuss.

The U.S. respondents' top concern is information transfer. In particular, the 2008 respondents are more concerned about disclosures of their purchasing patterns than the 2002 respondents ($p=0.0087$). Additionally, the 2008 respondents are now more concerned about the trading/selling of Personally Identifiable Information (PII) to third parties ($p=0.0013$).

The second privacy concern is notice/awareness. The 2008 respondents expressed a stronger desire to be notified about security safeguards being used to protect their PII than the 2002 respondents ($p=0.0029$). On the other hand, the 2008 respondents are less concerned about: options for deciding how their PII is used ($p<0.0001$); changes in privacy practices ($p<0.0001$); disclosures concerning PII use ($p=0.0144$); and previously undisclosed changes in the way that PII is used ($p=0.0002$).

The third and fourth concerns of U.S. respondents relate to information storage and access/participation. In contrast to the previous two categories, there were no significant changes in these two concerns from the 2002 survey to the 2008 survey. The fifth concern relates to information collection. When compared to the 2002 respondents, the 2008 respondents are more concerned about websites recording information regarding previously visited web sites ($p=0.0002$).

The respondents' sixth information privacy concern is personalization. The 2008 respondents are more concerned about their browsing experiences being customized in general ($p<0.0001$) and their purchasing patterns being monitored ($p<0.0001$). In addition, the respondents are more concerned about their PII being used for marketing or research activities ($p=0.0308$). However, the 2008 respondents are less concerned about the use of cookies ($p=0.0391$) than the 2002 respondents.

3. Changes in U.S. Privacy Concerns Since 2002

Our 2008 survey results suggest that individuals are more uncomfortable with companies, such as data brokers and credit bureaus, trading/sharing/selling PII with the companies with which they engage in business. It is likely that the previously mentioned increase in fraud and identity theft complaints being filed, as well as news stories pertaining to data brokers and data breaches [AHB04, OAB07], have contributed to this difference in the level of concern about information transfer. Since 2002, the press has been rife with stories about third party data use/transfers as well as data breach and identity theft reports. These stories have heightened public awareness about the existence of data brokers and their collection of information from public sources. Consider the January 2006 landmark Choicepoint FTC settlement in which the data broker agreed to pay $10 million in civil penalties and $5 million in consumer redress [OAB07]. News events, such as the Choicepoint case, may have contributed to the increased concern among the survey respondents with regard to the trading and selling of their PII to third parties.

The 2008 survey revealed that individuals' level of concern about notice/awareness has decreased. Although notice/awareness remains the second primary privacy concern among U.S. respondents, several factors may have contributed to this decrease in level of concern. It is possible that people are becoming desensitized to privacy notices (e.g., HIPAA privacy notices at healthcare facilities) and reports about data breaches to the point that they almost ignore them. In addition, recent studies have shown that privacy policies are burdensome and difficult for consumers to comprehend [MRK09, VEA08]. Another survey examined whether consumers read online privacy notices; 17% of the 2,468 respondents stated that they never read privacy notices [Cul03, CM01]. The survey found that privacy notices are considered too lengthy, include too much legalese, and are too difficult to read [Cul03, CM01]. Moreover, an

analysis of healthcare privacy notices before and after HIPAA's effective date revealed that healthcare privacy notices have become longer, more complex, and more difficult to comprehend post-HIPAA [AEV07]. An experiment that compared 993 individuals' perceptions about organizations' privacy policies versus their comprehension of those policies revealed that individuals perceive organizations with traditional natural language privacy policy representations to be the most secure yet the most difficult to comprehend [VEA08]. Individuals better comprehend other, more concise, formats over the commonly used natural language policy statements [VEA08]. Privacy scholars continue to recommend that privacy policies be written in a concise and comprehensible manner [AEV07, AEH04, Cul03, MRK09, VEA08] and among U.S. survey respondents, notice/awareness remains their second most important privacy concern.

The survey results reveal an increase in individuals' level of concern about information collection, specifically with regard to websites collecting information about previously visited websites. A similar practice that led to public outcry is the 2006 Facebook case in which members became aware of the fact that their Facebook actions were suddenly being tracked online and published.[15] Initially, users were not aware of this and when members learned of this practice, there was no option to shut down the feed. In response to complaints, Facebook changed the way in which feeds were handled, allowing members to opt out of this tracking activity feed. Information collection can lead to tracking. A recent study notes that individuals want to be informed about when websites track their online activities and want to have control over this tracking [GPS09]. The increased concern with websites that collect information about previously visited websites is especially pertinent today given that this information helps websites better place advertisements for targeted marketing and personalization.

Personalization occurs online when a website is customized, thus affecting the functionality or content offered to the user. Since the 2002 survey, individuals have become more concerned about personalization with regard to customized browsing experiences, monitored purchasing patterns, and targeted marketing and research. These concerns may be a result of increased attention to online behavioral advertising as well as the previously mentioned increase in e-commerce. Targeted marketing via online behavioral advertising, in particular, is receiving significant attention in the U.S. [SA08]. Through behavioral advertising, advertisements are targeted to individuals based on their online actions [MA10]. Our 2008 survey findings concerning personalization are especially relevant for policy makers given that Jon Leibowitz, FTC Commissioner, recently expressed that industry must demonstrate that it can self-regulate, following the FTC's behavioral advertising guidelines, or face "legislation by Congress and a more regulatory approach by our commission" [Cli09]. The increased attention to how companies are engaging in online behavioral advertising may have contributed to consumers' increased awareness and concerns about personalization in the 2008 survey.

4. Comparing U.S. and International Privacy Concerns

The 2002 survey did not yield a sufficient number of non-U.S. responses to warrant further examination for statistical significance, whereas the 2008 survey did. This enables us to examine any significant difference across both groups of respondents in the 2008 survey as we now discuss.

Our 2008 survey revealed that the U.S. and non-U.S. respondents share the same top three concerns; however, the top three concerns differ based on the order in which they are ranked. Recall that the U.S. respondents' top three concerns are: (1) information transfer, (2) notice/awareness, and (3) information storage. In contrast, the non-U.S. respondents' top three concerns are: (1) information transfer, (2) information storage, and (3) notice/awareness.

Across the board, information transfer is the top concern for both the U.S. and non-U.S. respondents; however, U.S. respondents are more concerned about information transfer than non-U.S. respondents.

[15] http://www.time.com/time/nation/article/0,8599,1532225,00.html

Specifically, individuals in the U.S. are more concerned about (a) the disclosure of their purchasing patterns and information to third parties; and (b) their personally identifiable information being traded with or sold to third parties.

The 2008 survey yielded 527 non-U.S. responses, 1,525 U.S. responses, and 42 responses in which country of residence was not specified. Although this provides an appropriate number of responses to compare differences between non-U.S. and U.S. responses, we must first account for any demographic differences between these two subsamples. Specifically, the non-U.S. respondents were, on average, 6 years older than the U.S. respondents. Because privacy perceptions between U.S. respondents in different age groups vary, we examine the privacy concerns of the non-U.S. and U.S. respondents in the 2008 survey by focusing our comparison within specific age groups. We limit our analysis and discussion herein to the 22-28, 29-35, 36-42, and 43-49 age groups because there were insufficient responses in the other age groups to warrant examination for statistical significance. We now discuss the significant differences within specific age groups across the non-U.S. and U.S. respondents as they relate to the privacy concerns dimensions.

The non-U.S. and U.S. survey respondents expressed different views about information transfer; specifically, within the younger age groups, the U.S. respondents are more concerned about information transfer than the non-U.S. respondents. U.S. respondents in the 22-28 age group are significantly more concerned about websites disclosing individuals' purchasing patterns to third parties. Similarly, U.S. respondents between ages 29-35 are significantly more concerned about general consumer information being shared with third parties. Finally with respect to information transfer, U.S. respondents in the 22-28 and 29-35 age groups are more concerned than their non-U.S. counterparts about PII being traded with or sold to third parties. Consider that citizens in India are generally unaware of incidents in which there PII is sold and/or traded among organizations [KC06]. In the past, citizens in India have been inclined to trust their PII will be used appropriately, but increasingly Indian press reports are raising awareness leading to a change in perceptions about trust [KC06]. In the EU, there is a general expectation that information will be protected and transferred according to law for approved purposes. For the U.S. to engage in global business, the U.S. Department of Commerce was required to develop the Safe Harbor[16] framework in response to EU concerns about transferring personal information from Europe to countries with inadequate privacy practices and laws. The EU approved the Safe Harbor framework in 2000. Given that citizens in India are generally more trusting about how their PII is sold and/or traded and that Safe Harbor was adopted to protect data about EU citizens when transferred to the U.S., it is not surprising that non-U.S. respondents are less concerned about the transfer of their personal information.

The differences across the non-U.S. and U.S. respondents in their concerns about notice/awareness and access/participation are minimal. The only significant notice/awareness difference we observed exists between the 22-28 non-U.S. and U.S. age groups. Specifically, the U.S. respondents feel significantly stronger about wanting a website to disclose how their PII will be used. With regard to access/participation, non-U.S. respondents in the 29-35 age group feel significantly stronger than their U.S. counterparts about wanting a website to allow individuals to check their PII for accuracy.

Differences in concerns about information storage across non-U.S. and U.S. respondents are solely within the 22-28 age group—the youngest of the analyzed age groups. The non-U.S. respondents in this age group are significantly more concerned about unauthorized employees and/or unauthorized hackers gaining access to their information. However, non-U.S. respondents in the other analyzed age groups agree with their U.S. counterparts with regard to information storage concerns.

The non-U.S. and U.S. respondents revealed different views about information collection. Non-U.S. respondents in the 36-42 age group are significantly more concerned about a website he/she visits

[16] http://www.export.gov/safeharbor/index.asp

collecting information about browsing patterns without an individual's consent. Similarly, non-U.S. respondents in the 22-28 age group are significantly more concerned about a website he/she visits collecting information about browser configurations or IP address, without an individual's consent. The European Union Article 29 Data Protection Working Party is an independent European advisory body with representation from each EU member state; it advises the EU Commission on the adequacy of data protection standards in non-EU countries. On February 10, 2009, this influential group adopted the stance that "IP addresses are commonly used to distinguish between users to whom should be applied a different treatment for example in the context of targeted advertisement serving or profile creation" [Art09]. In 2009, a federal judge in Seattle ruled that IP addresses are not personal information because an IP address identifies a computer not a person.[17] Given the differing definitions of IP addresses in the EU versus in the U.S., it is not surprising that the non-US respondents are more concerned about websites collecting information about web browser configurations and IP addresses.

Personalization is a more significant consideration for the non-U.S. respondents than for the U.S. respondents. Although the respondents in the 15-28, 29-35, 36-42, and 43-49 age groups among the non-U.S. respondents share a strong concern about PII use, concerns about using customer purchase history and cookies vary between specific age groups. The non-U.S. 15-28 and 43-49 age groups are significantly more concerned than their U.S. counterparts about using purchase history to customize browsing experiences. In contrast, the 29-35 non-U.S. age group is more concerned about cookies being used for customization.

5. Summary

It is important to understand that Internet users' still share the same primary privacy concerns today as in 2002. As with other privacy surveys, our respondents express concern about managing their personal information. Such disclosures occur despite the knowledge that individuals, in general, are increasingly engaging in a variety of Internet activities that require some kind of information exchange. While our analysis is based solely on individual responses, rather than individual actions, the information garnered with this study provides useful and practical recommendations.

A great deal has happened in the economic, legal, and cultural landscape over the course of six years. These events may account for the specific differences in users' levels of concern about privacy as discussed herein. Two specific findings are extremely relevant from a public policy perspective. First, the fact that U.S. respondents are more concerned about practices that lead to behavioral advertising today than in 2002 should be taken into account by policy makers at the FTC as well as Chief Privacy Officers at companies engaging in online behavioral advertising. In addition, the U.S. Congress recently held hearings about online behavioral advertising[18], which suggests that they are considering introducing legislation to regulate these activities. The findings of our 2008 survey highlight consumers' concerns about personalization. Lawmakers should take this into account when examining protections for individuals' online privacy. Second, the fact that non-U.S. respondents are more concerned about websites collecting IP addresses suggests that either the EU definition of IP addresses as personally identifiable has been generally accepted outside the U.S. and/or that the U.S. and EU need to engage in further discussion to achieve a mutually agreeable understanding to more readily facilitate cooperative global commerce.

Finally, authors of organizations' privacy notices should take into account that consumers want to know about their privacy practices. Any organizations' privacy notice should give special consideration to ensure that Internet users' top three primary privacy concerns are adequately addressed therein. An

[17] *Johnson v. Microsoft Corp*., 2009 WL 1794400 (wd Wash. June 23, 2009)

[18] http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1678:energy-and-commerce-subcommittee-hearing-on-behavioral-advertising-industry-practices-and-consumers-expectations&catid=129:subcommittee-on-commerce-trade-and-consumer-protection&Itemid=70

organization's published privacy notices may be seen as a signal about the trustworthiness of an organization and, clearly, there are three specific things that users are most concerned about and want to see addressed in a privacy notice [EAA05]. We are currently repeating our privacy notice content analysis study to examine how these notices have evolved since 2002 and to determine whether these privacy notices are better aligned with Internet users' privacy concerns. In addition, we plan to rerun the survey in a few years given that privacy awareness is on the rise around the world.

Acknowledgements

This project was funded by NSF ITR Grant # 0325269, NSF Cyber Trust Grant # 0430166 and Intel Corporation. In addition, IBM and Blue Cross Blue Shield of North Carolina provided participant prizes.

References

[AE04] A.I. Antón and J.B. Earp, "A requirements taxonomy for reducing web site privacy vulnerabilities," *Requirements Engineering Journal*, 9(3), pp. 169-185, 2004.

[AEH04] A.I. Antón, J.B. Earp, Q. He, W. Stufflebeam, D. Bolchini, and C. Jensen, "Financial Privacy Policies and the Need for Standardization," *IEEE Security and Privacy*, vol. 2, no. 2, pp. 36-45, Mar. 2004

[AEV07] A.I. Antón, J.B. Earp, M.W. Vail, N. Jain, C. Gheen and J.M. Frink, "HIPAA's Effect on Web Site Privacy Policies," *IEEE Security & Privacy*, 5(1), pp. 45-52, January/February 2007.

[AHB04] A.I. Antón, Q. He, and D. Baumer, "Inside JetBlue's Privacy Policy Violations," *IEEE Security & Privacy*, 2(6), pp. 12-18, November/December 2004.

[Art09] Article 29 Data Protection Working Party, "Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)," WP 159, February 10, 2009.

[Cli09] S. Clifford. "Many See Privacy on Web as Big Issue, Survey Says," *New York Times*, March 16, 2009.

[Cul03] M.J. Culnan, "How Privacy Notices Promote Informed Consumer Choice," in. P.J. Bruening (Ed), *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*, Washington: Center for Democracy & Technology, 2003.

[CM01] M. J. Culnan and G. R. Milne, "The Culnan-Milne Survey on Consumer and Online Privacy Notices: Summary of Responses," http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milney.pdf, December 2001.

[EAA05] J.B. Earp, A.I. Antón, L. Aiman-Smith, and W. Stufflebeam, "Examining internet privacy policies within the context of user privacy values," *IEEE Transactions on Engineering Management*, volume 52(2), pp. 227-237, May 2005.

[GPS09] J. Gomez, T. Pinnick, and A. Soltani, "KnowPrivacy" (June 1, 2009) http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

[KC06] P. Kumaraguru and L. Cranor, "Privacy in India: Attitudes and Awareness," in *Privacy Enhancing Technologies,* G. Danezis and D. Martin, eds., 2006.

[MA10] A.K. Massey and A.I. Antón, "Behavioral Advertising Ethics," in *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*, M. Dark, ed., In Press for Publication in 2010.

[MRK09] A.M. McDonald, R.W. Reeder, P.G. Kelley, and L.F. Cranor, "A Comparative Study of Online Privacy Policies and Formats," *Privacy Enhancing Technologies Symposium*, 2009.

[OAB07] P.N. Otto, A.I. Antón, and D.L. Baumer, "The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information," *IEEE Security and Privacy*, vol. 5, no. 5, pp. 15-23, Sep./Oct. 2007.

[SA08] P. Swire and A.I. Antón, "Online Behavioral Advertising: Technical Steps Needed to Ensure Consumer Control," Testimony for the Federal Trade Commission, in response to the FTC Staff Statement, Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, 10 April 2008.

[VEA08] M.W. Vail, J.B. Earp, and A.I. Antón, "An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies," *IEEE Transactions on Engineering Management*, 55(3), pp. 442-454, August 2008.

Appendix A - Summary Statistics for U.S. Respondents ONLY

	Item Statement	Mean		Standard Deviation		P value
		2002	2008	2002	2008	
Personalization	*I mind when a Web site uses my Personally Identifiable Information (PII) to customize my browsing experience.*	3.150	3.500	1.28	1.2	< 0.0001
	I mind when a Web site uses cookies to customize my browsing experience.	3.230	3.110	1.32	1.26	0.0391
	I mind when a Web site uses my purchasing history to personalize my browsing experience.	3.250	3.270	1.35	1.33	0.7259
	I mind when my PII (Personally Identifiable Information) is used for marketing or research activities.	4.120	4.220	1.1	1.01	0.0308
	I mind when a Web site monitors my purchasing patterns.	3.490	3.780	1.35	1.2	< 0.0001
	Average	3.448	3.576			
Notice / Awareness	*I want the option to decide how my PII is used.*	4.790	4.560	0.49	0.65	< 0.0001
	I want a Web site to disclose security safeguards used to protect my PII.	4.420	4.520	0.84	0.69	0.0029
	I want a Web site to disclose how my PII (Personally Identifiable Information) will be used.	4.750	4.690	0.52	0.56	0.0144
	I want a Web site to inform me before using my PII in a manner that it had not previously disclosed to me.	4.800	4.700	0.55	0.59	0.0002
	I want a Web site to keep me informed of changes to its privacy practices.	4.610	4.500	0.67	0.68	< 0.0001
	Average	4.674	4.594			
Transfer	*I mind when a Web site discloses my buying patterns to third parties.*	4.680	4.750	0.71	0.61	0.0087
	I mind when my information is shared with third parties.	4.740	4.770	0.61	0.57	0.2591
	I mind when my PII (Personally Identifiable Information) is traded with or sold to third parties.	4.820	4.890	0.54	0.41	0.0013
	Average	4.747	4.803			
Collection	*I mind when a Web site that I visit collects (without my consent) information about my browsing patterns.*	4.170	4.190	1.14	1.07	0.5572
	I mind when a Web site that I visit collects (without my consent) information about my browser configuration.	3.650	3.670	1.36	1.32	0.7801
	I mind when a Web site that I visit collects (without my consent) information about my IP address.	3.980	4.000	1.24	1.22	0.7677
	I mind when a Web site that I visit collects (without my consent) information about the type of computer/Operating System I use.	3.500	3.420	1.37	1.36	0.1513
	I mind when a Web site records the previous Web site I visited.	4.080	4.250	1.15	1.03	0.0002
	Average	3.876	3.906			
Info Storage	*I am concerned about unauthorized employees getting access to my information.*	4.480	4.450	0.84	0.82	0.4508
	I am concerned about unauthorized hackers getting access to my information.	4.590	4.610	0.76	0.71	0.4406
	Average	4.535	4.530			
A/P	*I want a Web site to allow me to check my PII (Personally Identifiable Information) for accuracy.*	4.380	4.340	0.96	0.8	0.2342
	I want a Web site to allow me to modify my PII.	4.380	4.340	0.96	0.81	0.3774
	Average	4.380	4.340			

Each item uses a 5-point Likert scale anchored by "Strongly Disagree" (1) and "Strongly Agree" (5).
A = April 5, 2002 to May 31, 2002 (n=827); **B =** August 11, 2008 to September 29, 2008 (n=1525)