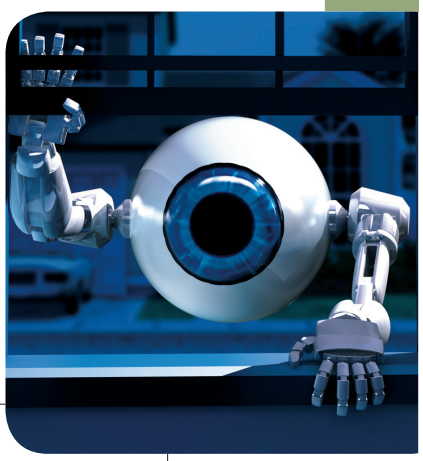
How Internet Users' Privacy Concerns Have Evolved since 2002

A 2008 survey revealed that US Internet users' top three privacy concerns haven't changed since 2002, but privacy-related events might have influenced their level of concern within certain categories. The authors describe their results as well as the differences in privacy concerns between US and international respondents.



Annie I. Antón, Julia B. Earp, and Jessica D. Young
North Carolina State University

Understanding and protecting personal privacy in information systems is becoming increasingly critical with widespread use of networked systems and the Internet. In 2002, we created and validated a survey instrument to establish a baseline of Internet users' privacy concerns.[1] We developed this instrument by using a subset of the Antón and Earp privacy goal taxonomy[2] to express dimensions of privacy concerns such as access/participation, information collection, information storage, information transfer, notice/awareness, and personalization.

The 2002 survey revealed that Internet users were primarily concerned about information transfer, notice/awareness, and information storage. We also learned that users' privacy concerns did not align with online privacy policies because the latter primarily emphasized data integrity/security, information collection, and user choice/consent. Thus, we found no overlap between the top three privacy concerns among Internet users and the items most emphasized in Internet privacy policies. In 2008, we repeated our survey to determine whether and how users' privacy interests have evolved in the six intervening years.

Then and Now

Many privacy-related events have occurred since 2002, prompting us to examine whether individuals' privacy concerns have evolved. We quickly learned that this also entailed considering how the environment has evolved as well. For example, the US Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996 but did not require compliance until 2003. Therefore, the compliance date occurred after our first survey but before the second; consequently, 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 was required to sign a statement indicating that they had received or read that organization's privacy notice.

The economic and legal landscape has also changed over the six years between our first and second surveys. Consider the US Census Bureau data that shows an increase in US e-commerce retail sales from $10.2 billion during the second quarter of 2002 to $31.6 billion during the third quarter of 2008 (www.census.gov/mrts/www/ecomm.html). Clearly, this increase in online shopping suggests that Internet users might be more comfortable sharing their sensitive financial information (such as credit-card numbers) with Web sites than they were six years ago.

Professional and social networking sites that let individuals connect with coworkers, friends, family, classmates, and others online have seen a similar jump in usage since 2002. LinkedIn, a professional networking site founded in May 2003, had 33 million users by October 2008 (http://press.linkedin.com/history). MySpace, founded in late 2003, had 110 million active users by January 2008 (www.web-strategist.com/blog/2008/01/09/social-network-stats-facebook-myspace-reunion-jan-2008/), and Facebook, launched in February 2004, had more than 100 million active users by August 2008 (www.facebook.com/press/info.php?timeline). These num-

Authorized licensed use limited to: Sterne Kessler Goldstein Fox. Downloaded on June 23,2025 at 12:23:28 UTC from IEEE Xplore. Restrictions apply.

Security Tech EX2013
Home Depot v. Security Tech
IPR2024-01420

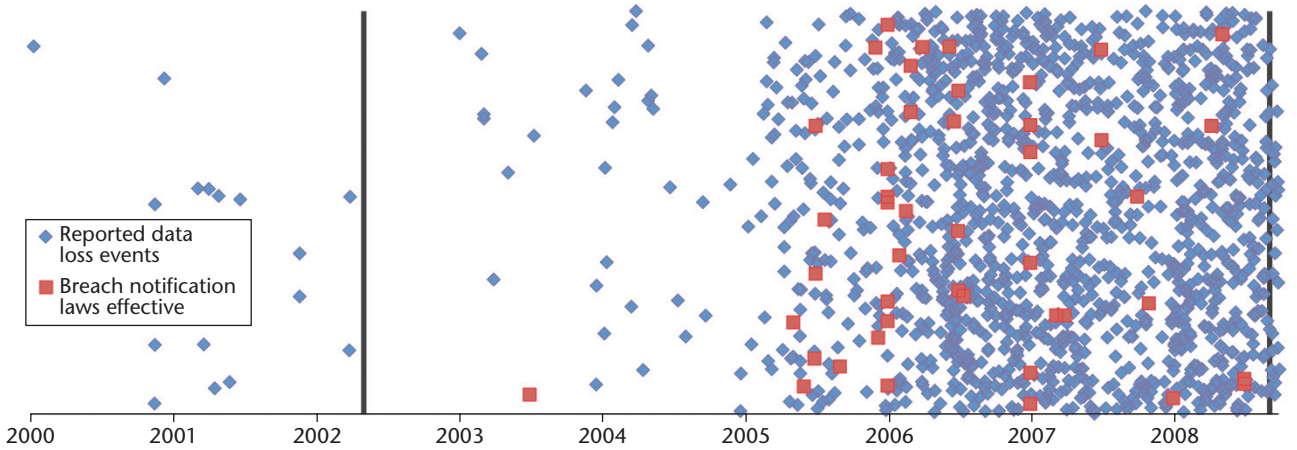


Figure 1. Breach notification laws and reported data loss events. Blue diamonds represent individual data loss events and red squares represent the effective date for the different state-based data breach notification laws. The gray vertical bars mark the times during which we conducted our surveys in 2002 and 2008. We generated this figure from http://datalossdb.org using data accessed on 20 April 2009.

bers indicate that people increasingly feel comfortable putting varied information about themselves online.

Individuals also appear more willing to speak out about what they perceive as invasions of privacy when engaging in online activities. For example, in February 2009, Facebook changed its Terms of Service regarding its information practices, resulting in a public outcry from its members that manifested in the creation of Facebook user groups protesting the change. In response to this outcry, Facebook reverted back to its previous terms while crafting a new version that reduced the problematic verbiage (http://blog.facebook.com/blog.php?post=54746167130).

Along with the increase in online shopping and professional/social networking, the number of consumer complaints about information practices has also risen. The US Federal Trade Commission's (FTC's) Consumer Sentinel Network has an online database of consumer complaints addressing, for example, fraud and identity theft (www.ftc.gov/sentinel). To better understand complaint trends, we examined the Consumer Sentinel Network Data Book, a summary of this consumer complaint database that contains statistics about complaints, descriptions of complaint categories, and sample complaints, as well as descriptions of Consumer Sentinel Network member organizations and how much information each contributes to the database.[3] The total number of annual complaints has continually increased each year, more than doubling since 2002, suggesting that people might be more aware 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 chronicled by the Privacy Rights Clearinghouse's *A Chronology of Data Breaches* using data from the Open Security Foundation's DataLossDB (http://datalossdb.org), which appears to be the most comprehensive list of data loss events available (www.privacyrights.org/ar/ChronDataBreaches.htm). The database had only 16 reported events before 2002, with no events reported during the course of our first survey. In contrast, at the start of the second survey, the database contained 1,370 reported events, and 47 additional events occurred during its course.

In response to concerns about the need to notify individuals about compromises of their sensitive information, states are passing data breach notification laws. In fact, as of this writing, Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota are the only US states without such laws, which vary by state but 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 1 July 2003; the next wave of 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 notification laws. We verified the laws' effective dates across at least two sources and combined them with data loss event dates from the previously mentioned DataLossDB. Blue diamonds represent individual data loss events, and red squares represent the effective dates for different state-based data breach notification laws. Gray vertical bars mark the times during which we conducted our surveys. 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.

In addition to data breach laws, most states now have security freeze laws to protect consumers from

Authorized licensed use limited to: Sterne Kessler Goldstein Fox. Downloaded on June 23,2025 at 12:23:28 UTC from IEEE Xplore. Restrictions apply.

identity theft. These laws allow consumers to put a hold on their credit files to avoid anyone else from being able to fraudulently open new accounts with stolen information. The first security freeze law went into effect in California in 2003. Today, Washington, DC, and 47 states (excluding Alabama, Michigan, and Missouri) have followed suit. These laws vary from state to state—for example, in Arkansas, Kansas, Mississippi, and South Dakota, the freeze applies only to identity theft victims who file a police report, whereas the other states allow any consumer to place a security freeze on his or her own account anyway. In 2007, the US 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 (www.worldprivacyforum.org/creditfreeze.html).

Survey Methodology and Results

The purpose for creating our original survey instrument in 2002 was to support our exploration into Internet users' privacy concerns.[1] Our analysis of more than 100 privacy notices in three domains—retail, finance, and healthcare—informed our development of the instrument.[4] We also used the information obtained from our content analysis of privacy notices to further examine how individuals' online privacy concerns align with what organizations express in their privacy policies. We grouped the survey statements (see the Web extra at www.computer.org/cms/Computer.org/dl/mags/sp/2010/01/extras/msp2010010021s.pdf) according to six dimensions of privacy concerns based on the following classifications—personalization, notice/awareness, information transfer, information collection, information storage, and access/participation;[1] a comprehensive description of each category appears elsewhere.[2] We ran the original survey from 5 April 2002 to 31 May 2002, producing 1,005 usable responses, with 827 of these responses representing individuals in the US.

The methodologies in the 2002 and 2008 surveys are the same with respect to the survey items and distribution process. The main difference is that the first effort included developing the survey instrument, so the methodology had more steps; the second survey already had a validated instrument with which to begin. The 2008 survey was available online from 11 August 2008 through 29 September 2008 and produced a total of 2,094 usable responses, with 1,525 of these responses representing individuals in the US, 527 representing individuals outside the US, and 42 indicating that the respondent chose "rather not say" for the country of primary residence. (Respondents did not have to answer all the questions in the 2002 survey, hence the "rather not say" option in the 2008 survey, which required responses for all questions.) We advertised the survey using a wide variety of mechanisms, including attaching fliers to bulletin boards around campus, posting announcements on academic Web sites and professional/social networking sites, and sending emails to our own personal and family networks.

The 2008 survey resulted in a much larger sample size, so we cannot compare two identical samples. However, the 2008 survey's demographics are similar to those of the 2002 survey—for example, most respondents were male in both surveys, and the largest participant group was the 22-to-28 age group. Most of the 2008 survey's US respondents reported having 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),[5] we can still make important inferences from this study. Furthermore, these demographics are comparable to profiles reported in other Internet user studies.[1]

As with any survey, there are always concerns about whether participants are completely honest when responding. We took several measures to avoid incorporating dishonest users' responses into the participant data set by removing responses that were deemed invalid. Additionally, we took necessary precautions to ensure that we preserved participant anonymity.

The 2008 survey revealed changes in Internet usage compared to 2002 respondents. For example, respondents in the 2008 study reported increased Internet usage overall ($p < 0.0001$), with most respondents spending more than 20 hours online a week. (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.) In 2002, 63.6 percent of respondents made online purchases once a month or less; in 2008, this number jumped to 78.8 percent—a statistically significant increase in online purchase frequency. In 2002, the only online activity in which more than 40 percent of respondents engaged was product purchasing; in contrast, 70 percent of the 2008 respondents engaged in education, financial services, product purchasing, and research activities.

Interestingly, in spite of all these increased numbers, our 2008 survey revealed that individuals' primary information privacy concerns had not changed since 2002; what *did* change was their level of concern. The top concern was still information transfer. In particular, the 2008 survey participants were more concerned about disclosures of their purchasing patterns than the 2002 respondents ($p = 0.0087$), but they were also concerned about the trading or selling of personally identifiable information (PII) to third parties ($p = 0.0013$). The second privacy concern was notice/awareness. Respondents to the 2008

Authorized licensed use limited to: Sterne Kessler Goldstein Fox. Downloaded on June 23,2025 at 12:23:28 UTC from IEEE Xplore. Restrictions apply.

survey expressed a stronger desire to be notified about the security safeguards being used to protect their PII than the 2002 respondents ($p = 0.0029$). On the other hand, the 2008 respondents were 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 ($p = 0.0002$).

US respondents' third and fourth highest concerns related to information storage and access/participation. In contrast to the previous two categories, we found no significant changes in these two concerns from the 2002 to the 2008 surveys. The fifth concern related to information collection. When compared to the 2002 respondents, the 2008 respondents were more concerned about Web sites' propensity to record information about previously visited sites ($p = 0.0002$). Finally, the respondents' sixth information privacy concern was personalization. The 2008 respondents were more concerned about their browsing experiences being customized in general ($p < 0.0001$) and their purchasing patterns being monitored ($p < 0.0001$). They were also more concerned about their PII being used for marketing or research activities ($p = 0.0308$). However, the 2008 respondents were less concerned about the use of cookies ($p = 0.0391$) than the 2002 respondents.

Changes in US 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, or selling PII with the other 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,[6,7] have contributed to this difference in the level of concern about information transfer. Consider the January 2006 landmark Choicepoint FTC settlement in which the data broker agreed to pay US$10 million in civil penalties and $5 million in consumer redress. Such news stories in particular have heightened public awareness about the existence of data brokers and their collection of information from public sources.

The 2008 survey also revealed that individuals' level of concern about notice/awareness decreased. Although notice/awareness remains the second primary privacy concern among US respondents, several factors might have contributed to this drop. For example, some people might have become desensitized to privacy notices (such as the financial privacy statements sent to customers at least once a year as required by law) 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.[8,9] One survey, for example, examined whether consumers read online privacy notices and found that 17 percent of the 2,468 respondents stated that they did not because such notices are too lengthy, include too much legalese, and are too difficult to read.[10,11] Likewise, 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.[9] To combat this, privacy scholars continue to recommend that privacy policies be written in a concise and comprehensible manner.[5,8-10,12]

Our survey results revealed an increase in individuals' level of concern about information collection—specifically, Web sites collecting information about previously visited sites. This concern is especially pertinent today, given that this information helps Web sites better place advertisements for targeted marketing and personalization. Once again, Facebook provides an example—in 2006, its members became aware that their Facebook actions were suddenly being tracked online and published (www.time.com/time/nation/article/0,8599,1532225,00.html). Initially, users were not aware of this, but when they found out, they quickly learned that they had no option to shut down the feed. In response to complaints, Facebook changed the way it handles feeds, letting members opt out of the tracking activity.

Personalization occurs online when a Web site is customized, thus affecting the functionality or content offered to the user. Since the 2002 survey, individuals have become more concerned about personalization in 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 rise in e-commerce activity. In particular, targeted marketing via online behavioral advertising—in which ads are targeted to individuals based on their online actions—is receiving significant attention in the US today.[13,14] Our 2008 survey findings on personalization are especially relevant for policy makers, given that Jon Leibowitz, FTC commissioner, recently expressed that industry must demonstrate that it can self-regulate or face "legislation by Congress and a more regulatory approach by our commission."[15] This extra attention paid to how companies engage in online behavioral advertising may have contributed to consumers' increased awareness and concerns about personalization in the 2008 survey.

Authorized licensed use limited to: Sterne Kessler Goldstein Fox. Downloaded on June 23,2025 at 12:23:28 UTC from IEEE Xplore. Restrictions apply.

Comparing US and International Privacy Concerns

The 2002 survey did not yield a sufficient number of non-US responses to warrant further examination for statistical significance, but the 2008 survey did. Although US and non-US respondents shared the same top three concerns, they ranked them in a different order. Recall that the top three concerns for US respondents were information transfer, notice/awareness, and information storage. In contrast, the non-US respondents' top three concerns were information transfer, information storage, and notice/awareness.

Although information transfer was the top concern for both US and non-US respondents, US respondents had an even higher level of concern about it than their non-US counterparts. Specifically, people in the US were more concerned about the disclosure of their purchasing patterns and information to third parties and their PII being traded with or sold to third parties.

The 2008 survey yielded 421 non-US responses (from 60 different countries), 1,525 US responses, and 148 responses in which participants did not specify country of residence. Most non-US responses represented India (34 percent), the EU (23 percent), and China (8 percent). Although this gave an appropriate number of responses to compare differences between non-US and US responses, we first had to account for any demographic differences between these two subsamples. Specifically, non-US respondents were, on average, six years older than US respondents. Because privacy perceptions between US respondents in different age groups vary, we examined the privacy concerns of the non-US and US respondents in the 2008 survey by focusing our comparison within specific age groups. We limited our analysis and discussion to the 22-to-28, 29-to-35, 36-to-42, and 43-to-49 age groups because there were insufficient responses in the other age groups to warrant examination for statistical significance.

Non-US and US survey respondents expressed different views about information transfer, especially within the younger age groups, with US respondents more concerned about it than non-US respondents. US respondents in the 22-to-28 age group were significantly more concerned about Web sites disclosing individuals' purchasing patterns to third parties. Similarly, US respondents between 29 and 35 were significantly more concerned about general consumer information being shared with third parties. Finally, US respondents in the 22-to-28 and 29-to-35 age groups were more concerned than their non-US counterparts about PII being traded with or sold to third parties.

Internet users in India are generally unaware of incidents in which their PII is sold or traded among organizations.[16] In the past, they have been inclined to trust that their PII will be appropriately used, but recent Indian press reports are raising awareness and driving a change in perceptions about trust.[16] In the EU, Internet users have a general expectation that their information will be protected and transferred according to law for approved purposes. For US companies to engage in global business, the US Department of Commerce had to develop the Safe Harbor framework in 2000 in response to EU concerns about transferring personal information from Europe to countries with inadequate privacy practices and laws (www.export.gov/safeharbor/index.asp). Given that India's citizens are generally more trusting about how their PII is sold or traded and that Safe Harbor was adopted to protect data about EU citizens as it is transferred to the US, it is not surprising that at least these two groups of non-US respondents were less concerned about the transfer of their personal information.

The differences across the non-US and US respondents in their concerns about notice/awareness and access/participation were minimal. The only significant notice/awareness difference we observed existed in the 22-to-28 age groups—specifically, US respondents felt significantly stronger about wanting a Web site to disclose how their PII would be used. With regard to access/participation, non-US respondents in the 29-to-35 age group felt significantly stronger than their US counterparts about wanting a Web site to allow individuals to check their PII for accuracy.

Differences in concerns about information storage across non-US and US respondents appeared solely within the 22-to-28 age group. Non-US respondents in this range were significantly more concerned about unauthorized employees or hackers gaining access to their information. However, non-US respondents in the other analyzed age groups agreed with their US counterparts on this particular concern.

Non-US and US respondents revealed different views about information collection. Non-US respondents in the 36-to-42 age group were significantly more concerned about a visited Web site collecting information about browsing patterns without an individual's consent. Similarly, non-US respondents in the 22-to-28 age group were significantly more concerned about a visited Web site collecting information about browser configurations or IP addresses without an individual's consent. The EU Article 29

Individuals have become more concerned about personalization in customized browsing experiences, monitored purchasing patterns, and targeted marketing and research.

Authorized licensed use limited to: Sterne Kessler Goldstein Fox. Downloaded on June 23,2025 at 12:23:28 UTC from IEEE Xplore. Restrictions apply.

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 10 February 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."[17] In 2009, a federal judge in Seattle ruled in *Johnson v. Microsoft Corp.* that IP addresses are not personal information because an IP address identifies a computer not a person. Given the differing definitions of IP addresses in the EU and the US, it is not surprising that non-US respondents were more concerned about Web sites collecting information about browser configurations and IP addresses.

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

Although the 50-to-57-year-old age group had insufficient responses, we can make some noteworthy observations for this group—in particular, for information transfer and notice/awareness. US respondents in this group were significantly more concerned about general consumer information being shared with third parties. In addition, they felt significantly stronger than their non-US counterparts about wanting to disclose security safeguards used to protect PII.

A great deal has happened in the economic, legal, and cultural landscape over the course of six years. These events could account for the specific differences we observed in users' levels of concern about privacy. Two specific findings are extremely relevant from a public policy perspective. First, policy makers at the FTC and chief privacy officers should take into account the fact that US respondents are more concerned about practices that lead to behavioral advertising today than they were in 2002. In addition, the US Congress recently held hearings about online behavioral advertising, suggesting that it's considering introducing legislation to regulate such activities (http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=e46b0d9f-562e-41a6-b460-a714bf370171). Second, the fact that non-US respondents are more concerned about Web sites collecting IP addresses suggests that either the EU definition of IP addresses as personally identifiable has been generally accepted outside the US or that the US 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 the fact that consumers want to know about their company's particular privacy practices. Users often interpret an organization's published privacy notices as a signal about the company's trustworthiness, and we've found evidence that users are concerned about three aspects in particular and want to see them addressed concisely and clearly.[1] We're currently repeating our privacy notice content analysis study to examine how these notices themselves have evolved since 2002 and to determine whether they are better aligned with Internet users' privacy concerns than they were in our earlier survey. In addition, we plan to rerun our survey in a few years, given that privacy awareness is on the rise around the world. ☐

Acknowledgments

US National Science Foundation (NSF) ITR grant number 0325269, NSF Cyber Trust grant number 0430166, and Intel funded this project. In addition, IBM and Blue Cross Blue Shield of North Carolina provided participant prizes.

References

1. J.B. Earp et al., "Examining Internet Privacy Policies within the Context of User Privacy Values," *IEEE Trans. Eng. Management*, vol. 52, no. 2, 2005, pp. 227–237.
2. A.I. Antón and J.B. Earp, "A Requirements Taxonomy for Reducing Web Site Privacy Vulnerabilities," *Requirements Eng. J.*, vol. 9, no. 3, 2004, pp. 169–185.
3. US Federal Trade Commission, "Consumer Sentinel Network Data Book for January-December 2008," Feb. 2009; www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf.
4. A.I. Antón, J.B. Earp, and A. Reese, "Analyzing Web Site Privacy Requirements Using a Privacy Goal Taxonomy," *Proc. 10th Anniversary IEEE Joint Requirements Engineering Conf.* (RE 02), IEEE Press, 2002, pp. 605–612.
5. A.I. Antón et al., "Financial Privacy Policies and the Need for Standardization," *IEEE Security & Privacy*, vol. 2, no. 2, 2004, pp. 36–45.
6. A.I. Antón, Q. He, and D. Baumer, "Inside JetBlue's Privacy Policy Violations," *IEEE Security & Privacy*, vol. 2, no. 6, 2004, pp. 12–18.
7. 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 & Privacy*, vol. 5, no. 5, 2007, pp. 15–23.
8. A.M. McDonald et al., "A Comparative Study of

Authorized licensed use limited to: Sterne Kessler Goldstein Fox. Downloaded on June 23,2025 at 12:23:28 UTC from IEEE Xplore. Restrictions apply.

Online Privacy Policies and Formats," *Proc. 9th Int'l Symp. Privacy Enhancing Technologies*, Springer Berlin/Heidelberg , 2009, pp. 37–55.

9. M.W. Vail, J.B. Earp, and A.I. Antón, "An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies," *IEEE Trans. Eng. Management*, vol. 55, no. 3, 2008, pp. 442–454.
10. M.J. Culnan, "How Privacy Notices Promote Informed Consumer Choice," *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*, P.J. Bruening, ed., Center for Democracy & Technology, 2003, pp. 12–16.
11. M.J. Culnan and G.R. Milne, "The Culnan-Milne Survey on Consumer and Online Privacy Notices: Summary of Responses," US Federal Trade Commission, 2001; www.ftc.gov/bcp/workshops/glb/supporting/culnan-milney.pdf.
12. A.I. Antón et al., "HIPAA's Effect on Web Site Privacy Policies," *IEEE Security & Privacy*, vol. 5, no. 1, 2007, pp. 45–52.
13. 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 Apr. 2008; www.americanprogress.org/issues/2008/04/pdf/swire_anton_testimony.pdf.
14. A.K. Massey and A.I. Antón, "Behavioral Advertising Ethics," to be published in *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*, M. Dark, ed., 2010.
15. S. Clifford, "Many See Privacy on Web as Big Issue, Survey Says," *The New York Times*, 16 Mar. 2009, www.nytimes.com/2009/03/16/technology/internet/16privacy.html.
16. P. Kumaraguru and L. Cranor, "Privacy in India: Attitudes and Awareness," *Privacy Enhancing Technologies*, G. Danezis and D. Martin, eds., Springer Berlin/Heidelberg, 2006, pp. 243–258.
17. "Opinion 1/2009 on the Proposals Amending Directive 2002/58/EC on Privacy and Electronic Communications (e-Privacy Directive)," Article 29 Data Protection Working Party, WP 159, 10 Feb. 2009.

Annie I. Antón *is a professor in the North Carolina State University College of Engineering, where she's the director of The Privacy Place. Her research interests include software requirements engineering, information privacy and security policy, regulatory compliance, software evolution, and process improvement. Antón has a PhD in computer science from the Georgia Institute of Technology. She's a distinguished scientist of the ACM as well as a member of the International Association of Privacy Professionals and a senior member of the IEEE. Contact her at aianton@ncsu.edu.*

Julia B. Earp *is an associate professor in the North Carolina State University College of Management. Her research interests focus on Internet security and privacy issues from several different perspectives, including data management, consumer values, systems development, and policy. Earp has a PhD in information technology from Virginia Tech. She's a member of the IEEE, the ACM, and the Association for Information Systems. Contact her via www4.ncsu.edu/~jbearp/.*

Jessica D. Young *is working toward a PhD in computer science at North Carolina State University. Her research interests include requirements engineering, privacy, and policy. Young has an MS in computer science from North Carolina State University. She's a member of the IEEE and the ACM. Contact her via www4.ncsu.edu/~jdyoung2.*

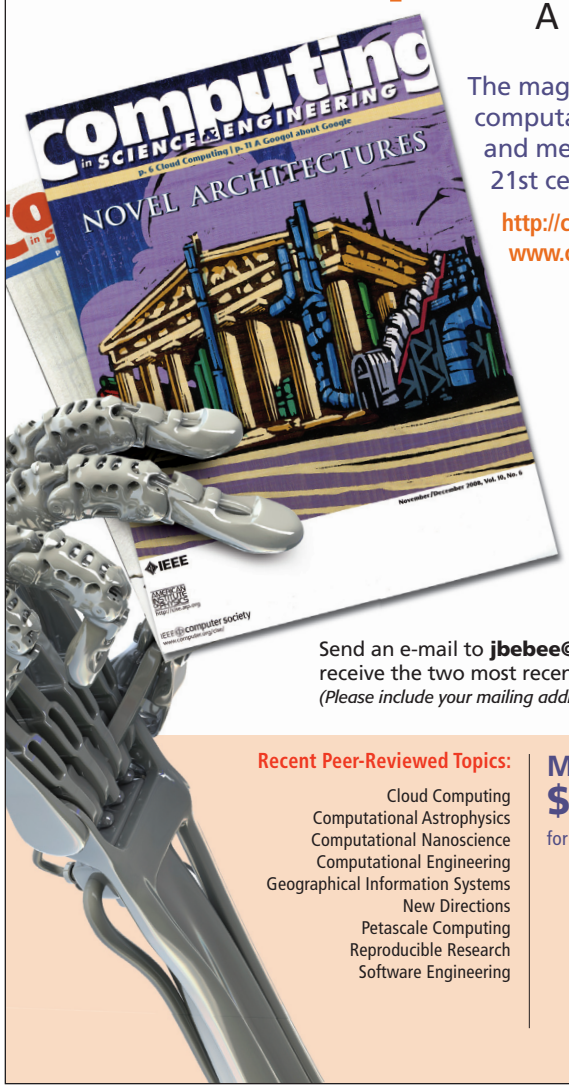
cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*

2 Free Sample Issues!

A $26 value

The magazine of computational tools and methods for 21st century science.

http://cise.aip.org
www.computer.org/cise



Send an e-mail to **jbebee@aip.org** to receive the two most recent issues of CiSE.
(Please include your mailing address.)

Recent Peer-Reviewed Topics:

Cloud Computing
Computational Astrophysics
Computational Nanoscience
Computational Engineering
Geographical Information Systems
New Directions
Petascale Computing
Reproducible Research
Software Engineering

MEMBERS
$47/year
for print & online

AIP
IEEE
IEEE computer society

Authorized licensed use limited to: Sterne Kessler Goldstein Fox. Downloaded on June 23,2025 at 12:23:28 UTC from IEEE Xplore. Restrictions apply.