BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Samuelson Law, Technology
& Public Policy Clinic

University of California, Berkeley
School of Law
396 Simon Hall
Berkeley, CA 94720
510-643-4800
510-643-4625 (fax)
http://www.samuelsonclinic.org/

[Submitted by email: privacy-noi-2010@ntia.doc.gov]

June 7, 2010

National Telecommunications Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Docket No. 100402174–0175–01, RIN 0660–XA12, Information Privacy and Innovation in the Internet Economy

Dear Messrs. Locke, Strickling, Sanchez, and Gallagher,

Thank you for soliciting comments on information privacy and innovation in the internet economy.

We wish to bring to your attention the rich and diverse scholarship of the Samuelson Law, Technology & Public Policy Clinic and of our colleagues at Berkeley Law who concentrate on information privacy issues.

The Samuelson Law, Technology & Public Policy Clinic at UC Berkeley School of Law gives law students the opportunity to collaborate with other graduate students and attorney faculty members in representing clients and the public interest on important and emerging issues in technology law. Established in January 2001, the Samuelson Clinic was the first in the nation to provide students with the opportunity to represent the public interest in sound technology policy through client advocacy and participation in legislative, regulatory, litigation and technical standard setting activities.

Today, the Samuelson Clinic functions as both a traditional legal Clinic and as a site of interdisciplinary, policy-relevant research. Much of this research is directly relevant to the Department's inquiry, and it is summarized below along with relevant research from our Berkeley Law colleagues. We hope that this information is helpful; please do not hesitate to contact us with questions or if we can be of further help.

Respectfully Submitted,

Jason Schultz
Director

Jennifer Urban
Director

Jennifer Lynch
Clinical Fellow

Chris Jay Hoofnagle
Senior Staff Attorney

Attachments (8)

- New smart meters are being installed in homes around California and the country provide much more data on energy customers than ever before--up to 750 to 3000 data points per month per household. Energy usage information of this granularity can reveal not only the various appliances that are consuming power within the household, but also their current operations. This radical departure from the traditional once-a-month manual readings can reveal specific household activities such as sleep, work, and travel habits and allows utilities and third parties with access to the information to "see" what is going on inside the home. The Samuelson Clinic, on behalf of its client the Center for Democracy & Technology, has submitted formal comments on the Smart Grid and information privacy to the Federal Trade Commission in its National Broadband Plan proceeding; to the National Institute of Standards and Technology in its Smart Grid Standards Framework proceeding;[1] and in conjunction with the Electronic Frontier Foundation to the California Public Utility Commissions' Smart Grid Rulemaking.[2] The comments urge the Commission to build strong privacy protections into the Smart Grid and to issue privacy protecting regulations based upon the Fair Information Practice principles.

- Media reports teem with stories of young people posting salacious photos online, writing about alcohol-fueled misdeeds on social networking sites, and publicizing other ill-considered escapades that may haunt them in the future. These anecdotes are interpreted as representing a generation-wide shift in attitude toward information privacy. Many commentators therefore claim that young people "are less concerned with maintaining privacy than older people are." In *How Different Are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies*, we found the picture to be far more nuanced than portrayed in the popular media.[3] In this telephonic (wireline and wireless) survey of internet using Americans (N=1000). Large percentages of young adults (those 18-24 years) are in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions. In several cases, there are no statistically significant differences between young adults and older age categories on these topics. Where there were differences, over half of the young adult-respondents did answer in the direction of older adults. There clearly is social significance in that large numbers of young adults agree with older Americans on issues of information privacy. We conclude that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data.

- Behavioral advertising is the subject of an international regulatory debate. Many advertisers have claimed that consumers want tailored advertising. However, in a national telephonic survey, we found that, contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%--say they would not want such advertising. In *Americans Reject Tailored Advertising and Three Activities that Enable It*,[4] we found that Americans favor much more vigorous privacy protections and severe penalties for violations of those protections. Further, we found a high degree of confusion about the protections that US law offers

---

[1] Comments of the Center for Democracy & Technology on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy, Docket Number 0909301329-91332-01. Available at http://www.cdt.org/content/cdt-comments-nist-smart-grid And Requirements

[2] Joint Comments of the Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining to the Smart Grid. Available at http://www.law.berkeley.edu/7973.htm

[3] Chris J. Hoofnagle et al., *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*, SSRN ELIBRARY (2010), http://ssrn.com/paper=1589864.

[4] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN ELIBRARY (2009), http://ssrn.com/paper=1478214.

consumers—most Americans mistakenly believe that privacy laws strongly limit information use.

- Despite the passage of sweeping financial services modernization and preemptive credit reporting legislation, identity theft still affects about 10 million Americans each year. In *Internalizing Identity Theft*,[5] Chris Hoofnagle finds in an empirical study of identity theft victims that credit grantors ignored obvious signs of fraud (and sometimes explicit warnings) on applications. Identity theft is the result of business incentives that prioritize quick credit granting over the avoidance of fraud. Of course, all businesses must find some reasonable balance between procedures and the avoidance of fraud, but the current identity theft landscape leaves victims with some costs of the crime—most notably in lost time. Hoofnagle proposes a system for credit grantors to compensate victims directly for out-of-pocket costs and lost time costs, because credit grantors are the least cost avoiders, because consumers cannot effectively insure against fraud, and because credit grantors are fully in control of the decision to issue a new account.

- In *Privacy on the Books and on the Ground*, Professors Ken Bamberger and Deirdre Mulligan explain that ambiguity is a *benefit* of the U.S. privacy framework.[6] Privacy law "on the ground" has benefitted from this ambiguity, because in order to manage shifting consumer expectations and regulator interests, companies have devoted significant resources to privacy management. This has resulted in the creation of C-level privacy officers in major companies, the professionalization of privacy officers, and the desire to satisfy the "soft law" of consumers privacy norms. Eliminating ambiguity from this system would likely result in more formalism and less substance—a world of "click through if you 'consent' to the privacy policy" approach.

- There have been many proposals to unify privacy law at the federal level, despite the historical role of states in consumer protection matters. Preemption is difficult policy issue, with all sides choosing positions that are outcome based, and frequently changing their attitude towards state legislation in different but similar contexts. In *Preemption and Privacy*, Paul Schwartz brings much light to this debate.[7] Schwartz clarifies where federal preemption can benefit regulation, such as where legislation can create field definitions to lower compliance costs. At the same time, Schwartz explains that the federalism "toolkit" contains many more options than ceiling or floor preemption—including options that allow a single state to create new privacy laws, preemption that is limited to "conduct" rather than the entire subject matter of the law, and creating sunsets on preemption that give industries and regulators incentives to regularly revisit the rules.

- The large majority of consumers believe that the term "privacy policy" describes a baseline level of information practices that protect their privacy. In short, Americans believe "privacy," like "free" before it, has taken on a normative meaning in the marketplace. When consumers see the term "privacy policy," they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information. In *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, Joseph Turow, Chris Hoofnagle, Deirdre Mulligan, Nathaniel Good, and Jens Grossklags argue that because the term "privacy policy" has taken on a specific meaning in the marketplace and connotes a particular level of protection to consumers, the Federal Trade Commission

---

[5] Chris Jay Hoofnagle, *Internalizing Identity Theft*, SSRN ELIBRARY, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1585564#.

[6] Bamberger, Kenneth A. and Mulligan, Deirdre K., Privacy on the Books and on the Ground. Stanford Law Review, Vol. 63, 2010; UC Berkeley Public Law Research Paper No. 1568385. Available at SSRN: http://ssrn.com/abstract=1568385

[7] Schwartz, Paul M., Preemption and Privacy. Yale Law Journal, 2009; UC Berkeley Public Law Research Paper No. 1404082. Available at SSRN: http://ssrn.com/abstract=1404082

("FTC") should regulate the use of the term "privacy policy" to ensure that companies using the term deliver a set of protections that meet consumers' expectations and that the term "privacy policy" does not mislead consumers during marketplace transactions.[8]

- Spyware is software that monitors user actions, gathers personal data, and/or displays advertisements to users. While some spyware is installed surreptitiously, a surprising amount is installed on users' computers with their active participation. In *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, authors Nathaniel S. Good, Rachna Dhamija, Jens Grossklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan report on results of an experiment in which 31 users conducted computer configuration tasks and passed a thorough interview process. The results suggested that mutual assent, in the legal sense, is largely unachievable given the current state of notices and law.

[8] J Turow et al., *The Federal Trade Commission and Consumer Protection in the Coming Decade*, 3 I/S J. OF LAW & POLICY 723 (2007), http://www.is-journal.org/V03I03/Turow.pdf.