Comments of the Privacy Rights Clearinghouse

Information Privacy and Innovation in the Internet
Docket No. 101214614-0614-01
RIN 0660-XA22

Department of Commerce
Office of the Secretary
National Telecommunications and Information Administration
International Trade Administration
National Institute of Standards and Technology

January 28, 2011

The Privacy Rights Clearinghouse (PRC) respectfully submits the following comments to the Department of Commerce for its consideration with respect to the "Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework" green paper.

Background

The Privacy Rights Clearinghouse is a nonprofit organization, established in 1992 and located in San Diego, California. It has a two-part mission: consumer education and consumer advocacy. The PRC has published more than 50 guides, called "Fact Sheets." [1] These Fact Sheets provide a wealth of practical information on strategies that consumers can employ to safeguard their personal information.

The PRC also invites individuals to contact the organization with their questions, concerns and complaints. Over the course of our 19-year history, PRC staff members have communicated directly with tens of thousands of consumers. The comments set forth in this document largely reflect our observations gathered from direct contact with individual consumers over the years. What we have learned from individuals forms the basis of our policy positions.

General Statements

The PRC believes that public discourse of personal privacy is exceedingly valuable, and appreciates that it is the subject of recent reports like Department of Commerce green paper as well as the Federal Trade Commission preliminary staff report.[2] However, the

[1] *See* PRIVACY RIGHTS CLEARINGHOUSE, FACT SHEETS, http://www.privacyrights.org/Privacy-Rights-Fact-Sheets (last visited Jan. 27, 2011).

[2] *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT, Dec. 2010.

Department has a very limited history of consumer protection,[3] and the PRC strongly believes that if it receives and asserts increased power in a manner that marginalizes the Federal Trade Commission's consumer protection role, individuals will not be well served.

As the Department notes in its report, consumer trust is crucial to the success of online commerce and necessary to further technological advancement.[4] Privacy Rights Clearinghouse agrees wholeheartedly with this statement. Unfortunately, many key privacy entities in the expanding marketplace for personal information have not sufficiently addressed the importance of consumer awareness, individual control, and choice when it comes to the use of a consumer's personal data. The result is that many consumers feel insecure about their personal privacy and safety on the Internet, and the clear solution is the creation of enforceable rules.

Privacy Rights Clearinghouse has based its work over the past 19 years on our interactions with individual consumers, and we find that consumer insecurity is grounded in numerous occurrences where personal information is exposed in ways that place people at risk.[5] Therefore, noting that consumer trust is pivotal to commercial success online, and that it has diminished with industry self-regulatory practices, PRC advocates comprehensive federal FIPPs-based data privacy legislation. The Fair Information Practice Principles are internationally recognized and provide underlying policy for many laws addressing individuals' information privacy. "Privacy laws in the United States, which are much less comprehensive in scope than laws in some other countries, often reflect some elements of FIP[P]s but not as consistently as the laws of other nations."[6]

---

[3] *See generally* THE WORLD PRIVACY FORUM, THE U.S. DEPARTMENT OF COMMERCE AND INTERNATIONAL PRIVACY ACTIVITIES: INDIFFERENCE AND NEGLECT, Nov. 22, 2010, *available at* http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf .

> The history of [the US Department of Commerce's forays into privacy] reveals the Department's primary focus, which is protecting business interests. This is not an unexpected outcome given the Department's goals and purpose. However, in looking at the potential for a broader role for the US Department of Commerce in privacy matters, an analysis of the Department's past history does not suggest that consumer protection has ever been a significant concern or priority. The Department's past history also indicates a lack of rigor regarding enforcement and compliance in the privacy programs it administers.

Id. at 2.

[4] DEPARTMENT OF COMMERCE, INFORMATION PRIVACY AND INNOVATION IN THE INTERNET ECONOMY, Dec. 15 2010, at 15, *available at* http://www.ntia.doc.gov/frnotices/2010/FR_IPTFPrivacy_RequestforComments_12162010.pdf .

[5] One example of this that PRC has seen many times is domestic violence victims whose personal information is readily available online at a time when they are striving for anonymity for personal safety reasons.

[6] Robert Gellman, *Fair Information Practices: A Basic History, Version 1.81,* May 13, 2020, *available at* http://bobgellman.com/rg-docs/rg-FIPshistory.pdf .

Accordingly, PRC discourages the Department of Commerce's proposal that the U.S. attempt to lead international privacy policy in a direction of voluntary enforceable codes. Rather than attempt to change and weaken privacy standards on the international stage, the U.S. would be better served by implementing both legislation and policies that work alongside those of countries that have already enacted more effective comprehensive privacy legislation.[7]

Summary of Recommendations and Questions for Further Discussion

1. The Task Force recommends adoption of a baseline commercial data privacy framework built on an expanded set of Fair Information Practice Principles (FIPPs).

a. Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or through other formal means to address how current privacy law is enforced?

FIPPs should be codified in a comprehensive national privacy law so the principles are enforceable against entities that violate them. The Department report acknowledges that the framework it discusses "does not involve a full right to control." "Instead, this framework articulates rights and obligations in personal information, such as a right to access and correct information about oneself and an obligation to use personal information only for specified purposes."[8] PRC strongly advocates for the inclusion of an individual right to control the use of personal data and supports public policy that strives to give consumers such effective control. Examples of comprehensive FIPPs that PRC supports as furthering the goal of consumer privacy and consumer control over personal data include both the OECD and Canada.[9]

b. How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement actions?

Baseline privacy principles should be enforced by the FTC. However, PRC recognizes that the FTC is currently underfunded and understaffed.

---

[7] For example, Canada's Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 [hereinafter PIPEDA]. EU Data Protection Directive 95/46/EC.

[8] U.S. DEPARTMENT OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK, GREEN PAPERS, DYNAMIC PRIVACY FRAMEWORK, Dec. 15, 2010, at 10 FN 17, *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf .

[9] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html; Personal Information Protection and Electronic Documents Act, *available at* http://laws.justice.gc.ca/en/ShowDoc/cs/P-8.6//20090818/en?page=1 .

Ideally, an independent federal privacy agency should be established in the U.S. that would operate much like the data protection commissions in the European nations, Canada, and many other countries around the world. Until such an agency is established, the FTC should be sufficiently funded and staffed to enforce a comprehensive national privacy law based on the FIPPs.

Furthering the discussion, PRC believes the term "voluntary enforceable" as related to codes of conduct concerning data privacy is an oxymoron. It is only under comprehensive baseline legislation and consistent effective enforcement that entities will gain consumer trust and operate under the proposed set of FIPPs. The Direct Marketing Association's enforcement mechanism is a prime example.[10] Because the enforcement mechanism is rarely used to expose businesses, and is not very visible to consumers, it does little to promote trust. This framework also does little to encourage entities to follow its Ethical Guidelines because companies are rarely exposed. The DMA publishes public information regarding complaints only under limited circumstances, and even then it is still on a permissive rather than mandatory basis.[11]

In fact, in the past two annual ethics reports published by the DMA, there have been only five companies whose cases were made public out of 58 cases reviewed by the Ethics Operating Committee, and none of those companies exposed were DMA members.[12] To the PRC, these facts both illustrate that it is difficult to ensure voluntary participation in such an ethics code, and that the DMA has not published any information on cases or complaints involving members. This quiet enforcement process does very little to instill trust in consumers that the DMA is honestly addressing all ethical concerns.

---

[10] *See generally* Direct Marketing Association, Complaint Handling Process and How to file a Complaint, http://www.the-dma.org/guidelines/complaintprocedures.shtml (last visited Jan. 27, 2010).

[11]

> Complaints referred to the Committee are reviewed against the Guidelines for Ethical Business Practice and if a majority of Committee members believe there is a potential violation, the company is contacted. Most companies work with the Committees to cease or change the questioned practice. Case proceedings are kept strictly confidential. However, if a member company does not cooperate and the Committees believe there are ongoing guidelines violations, the Committees can recommend that action be taken by the Board of Directors and can make case results public. Board action could include censure, suspension or expulsion from membership, and the Board may also make its actions public. If a non-member or a member company does not cooperate with the Committees and the Committees believe violations of law may also have occurred, referral of the case is generally made to federal and/or state law enforcement authorities for their review; such referral may be made public.

Direct Marketing Association, Complaint Handling Procedures and How to File a Complaint, http://www.the-dma.org/guidelines/complaintprocedures.shtml (last visited Jan. 27, 2010).

[12] *See* Direct Marketing Association, ETHICS CASE REPORT FEB. 2009–FEB. 2010, *available at* http://www.the-dma.org/guidelines/DMAEthicsCaseReport2-09-2-10-Final.pdf ; DMA, REPORT ON ETHICS COMMITTEE FINDINGS JULY-DECEMBER 2009, *available at* http://www.the-dma.org/guidelines/ethicscasereport1_09.pdf .

d. Should baseline commercial data privacy legislation include a private right of action?

Consumers should be able to bring a private right of action under any proposed baseline commercial data privacy legislation. The ability to bring a class action would allow consumers with monetarily insignificant but valid claims to band together and provide incentive to commercial entities mishandling data to comply with the FIPPs-based regulations. If it is worth it to breach the regulations for financial gain due to lax enforcement or insignificant penalties, commercial entities probably will.

2. To meet the unique challenges of information intensive environments, FIPPs regarding enhancing transparency; encouraging greater detail in purpose specifications and use limitations; and fostering the development of verifiable evaluation and accountability should receive high priority.

a. What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.

Privacy Rights Clearinghouse believes that enacting legislation with baseline requirements requiring transparency is the best means to ensure that entities present privacy policies in a manner in which consumers may more easily make informed choices. Legislation would provide clear incentives to entities using consumer data, and would ideally encompass a wide variety of entities not currently regulated by other privacy-related legislation (for example HIPAA, GLB or the FCRA).

Privacy Rights Clearinghouse expressly advocates against voluntary private sector approaches to promoting transparency. First, there is no way to ensure one hundred percent participation among entities if participation is voluntary. There are likely to be companies who adopt voluntary codes only in part, and others who opt out because compliance with a voluntary code is not worth it within their business model. Second, under clear baseline legislation encompassing FIPPs, it will be possible to keep pace with changing technologies. If a voluntary private sector approach is taken, changes could easily be enacted and consumers may not be aware of what privacy measures to assume apply to their online actions. This would do nothing to establish consumer trust in companies to whom they entrust their data. It is better for consumer protection that baseline legislation is enacted than to allow industry to create voluntary approaches and create a need to legislate later based on harm that is likely to occur under a voluntary code.

b. What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs (privacy impact assessment), to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?

As stated above, the PRC believes that the best manner to ensure that entities develop and adopt practical mechanisms to protect consumer privacy is through legislation. An example of consumer-friendly legislation that has not hindered online industry is California's Online Privacy Protection Act of 2003.[13] Operators of commercial websites or online services that collect personal information on California residents through a website must conspicuously post a privacy policy on the site and comply with the policy. This privacy policy must identify the categories of personally identifiable information collected about the site visitors and the categories of third parties with whom the operator may share the information. An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy.[14]

f. What are consumers' and companies' experiences with systems that display information about companies' privacy practices in contexts other than privacy policies?

PRC supports the use of just-in-time privacy notices that are displayed at or near the time when the consumer makes a decision or is about to disclose personal information. The notice could be in the form of a pop-up screen, or in any other feasible form as long as it is not buried in lengthy and jargon-filled privacy policy. The just-in-time approach is an excellent way to alert individuals to key relevant components of a privacy policy.

l. What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?

So that companies are encouraged to state clear, specific purposes for using personal information, there must be adequate enforcement of well drafted legislation.

m. How should purpose specifications be implemented and enforced?

If an individual's personal information is used in ways contrary to the purpose stated by the entity, the individual should be able to submit a complaint to the appropriate consumer protection agency, for example, the Federal Trade Commission. The FTC would also enforce such violations.

For such a consumer complaint process to be effective, there must be significant public outreach to let consumers know that it exists. The process itself must be user-friendly and include an easily navigable website.

Another strategy that would provide companies with incentive to comply with their stated purposes is to create a private right of action.

[13] *See* CA Bus. and Professions Code sections 22575-22579 (Online Privacy Protection Act of 2003).

[14] Cal. BUS. & PROF. CODE § 22575.

3. Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs. To encourage the development of such codes, the Administration should consider a variety of options, including (a) public statements of Administration support; (b) stepped up FTC enforcement; and (c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multi-stakeholder processes.

Privacy Rights Clearinghouse disagrees with the concept promoting the development of voluntary, enforceable codes of conduct first and foremost, and considers the idea to be contradictory. Over-arching comprehensive legislation will be more effective in ensuring uniform participation than creating a safe harbor framework where entities may opt to comply. However, PRC does agree that FTC enforcement should be stepped up with increased funding and staff devoted to that function. And, as stated above, the PRC believes that an independent privacy agency must ultimately be established in the U.S. for truly meaningful consumer privacy protection to be implemented and enforced.

4. Using existing resources, the Commerce Department should establish a Privacy Policy Office (PPO) to serve as a center of commercial data privacy expertise. The proposed PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together; and it would work in concert with the Executive Office of the President as the Administration's lead on international outreach on commercial data privacy policy. The PPO would be a peer of other Administration offices and components that have data privacy responsibilities; but, because the PPO would focus solely on commercial data privacy, its functions would not overlap with existing Administration offices. Nor would the PPO would have any enforcement authority.

Privacy Rights Clearinghouse discourages the creation of a PPO and finds it difficult to imagine that the fact that a PPO would focus solely on commercial data privacy precludes such an office from overlapping with existing administrative agencies. Commercial data privacy and consumer privacy interests almost always overlap, and the Department of Commerce is not equipped to address consumer protection. The Department represents the interests of industry rather than individual consumers, and it would be dangerous to take privacy policy-making from the more consumer-oriented FTC and effectively limit it to enforcement after consumers have been harmed.

Also, the multi-stakeholder process that the report suggests cannot realistically be expected to result in the development of meaningful consumer protection. Compromise is the name of the game in multi-stakeholder policy development processes, and consumers' privacy rights are far too important to be compromised away in such a process.

> **a. Should the FTC be given rulemaking authority triggered by failure of a multi-stakeholder process to produce a voluntary enforceable code within a specified time period?**

The FTC's rulemaking authority should be expanded but authority should not be conditioned on failure of a multi-stakeholder process to produce a so-called voluntary enforceable code. Again, PRC does not endorse a voluntary enforceable code. Who would have the power to decide the time period and whether there was a failure to produce a code? Also, how would the time period be determined, and how would failure be defined?

b. How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?

The Department must first fully support "Do Not Track" mechanisms, and understand the importance of protecting consumers and ensuring that they are able to make meaningful choices regarding online behavioral advertising. Privacy Rights Clearinghouse fully supports "Do Not Track," and recommends that the Department embrace the fact that the consumer benefits of such a system outweigh any monetary concerns of industry.

c. Under what circumstances should the PPO recommend to the Administration that new policies are needed to address failure by a multi-stakeholder process to produce an approved code of conduct?

Privacy Rights Clearinghouse would predict inevitable failure by such a multi-stakeholder process. As stated above in response to preceding questions, PRC does not consider any voluntary code to be a mechanism that would result in true privacy protection. Therefore PRC cannot specifically address how to quantify failure to determine whether it is substantial enough to recommend adopting new policies.

5. The FTC should remain the lead consumer privacy enforcement agency for the U.S. Government.

a. Do FIPPs require further regulatory elaboration to enforce, or are they sufficient on their own?

The FIPPs do require further regulatory elaboration, and while meaningful, they are not sufficient standing alone. Privacy Rights Clearinghouse believes that this should be in the form of comprehensive baseline legislation.

c. Should FIPPs be considered an independent basis for FTC enforcement, or should FTC privacy investigations still be conducted under Federal Trade Commission Act Section 5 "unfair and deceptive" jurisdiction, buttressed by the explicit articulation of the FIPPs?

FIPPs should be considered an independent basis for FTC enforcement in addition to Section 5 jurisdiction for "unfair and deceptive" practices. Instead of having to force a FIPPs violation into the category of either unfair or deceptive, it would be better to pursue privacy concerns under a framework designed with consumer privacy in mind. If FIPPs are unenforceable, they lose much of their meaning.

e. At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval? Potential options include providing an ex ante "seal of approval," delaying approval until the code is in use for a specific amount of time, and delaying approval until enforcement action is taken against the code.

The PRC does not view the development of a voluntary code as a viable means to protect personal privacy. If such a voluntary code were to be developed, it would not be appropriate for the FTC, in our opinion, to give its "seal of approval." An agency whose mission is consumer protection should not endorse a process that is inherently flawed vis-à-vis comprehensive privacy protection of American consumers.

7. Consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Such a framework should track the effective protections that have emerged from State security breach notification laws and policies. What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?

Privacy Rights Clearinghouse advocates enactment of baseline legislation with respect to commercial data security breaches. In particular, PRC supports California's model of Security Breach Notice codified in CA Civil Code sections 1798.29, 1798.82, and 1798.84. California's law requires a business that maintains unencrypted computerized data that includes personal information notify a California resident whose information was or is reasonably believed to have been acquired by an unauthorized person. The relevant information includes an individual's name plus one or more of the following: Social Security number, driver's license or California Identification Card number, financial account number, medical information or health insurance information.[15] New York has a similar law that requires notice for almost any breach regardless of a business' perceived risk.[16] Privacy Rights Clearinghouse believes it is better to have a defined notice requirement than to allow businesses to make a judgment call about whether a breach would adversely affect an individual.

Privacy Rights Clearinghouse supports general legislation that creates a baseline standard which individual states may go beyond and does not generally support preemption in the creation of security breach notice legislation unless the law is sufficiently strong.

8. A baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans, but rather should act in concert with these protections. Are there lessons from sector-specific

[15] Cal. CIV. CODE §§ 1798.29, 1798.82, 1798.84.

[16] *See* N.Y. GEN. BUS. LAW § 899-aa.

commercial data privacy laws—their development, their contents, or their enforcement—that could inform general U.S. commercial data privacy policy?

Although not perfect, the Fair Credit Reporting Act has many positive aspects that may help inform the creation and implementation of U.S. commercial data privacy policy. Although the FCRA is the oldest federal privacy law, it has maintained its relevance. Also, the FCRA provides an example of the effectiveness of FIPPs-based legislation. It provides a right of access, embodies purpose specification, enables correction of data, and so on.[17]

In terms of concerns, FCRA enforcement depends in large part upon the resources of the FTC. Because additional enforcement capabilities are necessary regardless of the form of either legislation or any implemented industry code, it is important to ensure that the FTC is both funded and staffed adequately.

9. Any new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.

a. Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving States free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

Privacy Rights Clearinghouse advocates against preemption of state laws, especially in the form of a broad preemption provision. Any preemption provision should be extremely narrow and set a baseline from which states may legislate and regulate new or unique concerns.

The following example from our own case files speaks to the importance of enabling states to continue to legislate on behalf of consumers' privacy rights. In the early 1990s the PRC assisted many identity theft victims. We observed the difficulty victims had in obtaining copies of the fraudulent credit card applications from credit issuers. Victims needed such documents to prove they themselves had not submitted them, showing, for example, that the signature was not theirs. But credit issuers resisted providing such documentation to victims. PRC and others advocated on behalf of consumers in the California Legislature, and subsequently California enacted legislation requiring credit card companies to enable consumers to obtain copies of their credit applications. This provision eventually was included in the FACT Act, becoming federal law.[18] It is

[17] *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 *et. seq.* (2000).

[18] Fair and Accurate Transaction Act of 2003 (FACTA), 15 U.S.C. § 1681 et. seq. (2003).

examples like this, where a state was able to respond to citizens' specific concerns, which illustrate the necessity to restrict preemption to very narrow instances.

b. How could a preemption provision ensure that Federal law is no less protective than existing State laws? What are useful criteria for comparatively assessing how protective different laws are?

Any federal law enacted must be sufficiently strong to ensure that it is no less protective than existing state laws. To compare how protective different laws are, it would be necessary to perform an analysis of all fifty states' laws.[19]

Another way in which to examine protectiveness is to analyze case law under the different laws. Whether case law is rich or non-existent is one indicator of the strength and protectiveness of the legislation. After analyzing and comparing the laws, the body drafting the legislation could arrive at a set of provisions that embody the strongest among the laws.

c. To what extent should State Attorneys General be empowered to enforce national FIPPs-based commercial data privacy legislation?

State Attorneys General should always be empowered to enforce national FIPPs-based data privacy legislation.

d. Should national FIPPs-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?

National FIPPs-based commercial data privacy legislation should not preempt State unfair and deceptive trade practices laws. Industry typically supports federal preemption in the case of consumer protection. The more claims preempted by federal law, the better for industry. This is true because there is typically no private right of action associated with federal consumer claims.

For example, if a company violates a privacy provision under state law it can be enforced by private citizens and state Attorneys General and District Attorneys. If there were preemption of state consumer protection laws, who would be responsible for enforcement absent the creation of a private right of action? Preemption goes against the concept of reducing federal intervention in matters that have typically been the subject of state law, and undermines the significant role private enforcement plays in ensuring consumers are protected against privacy violations.

[19] *See e.g.* NATIONAL CONFERENCE OF STATE LEGISLATURES, STATE SECURITY BREACH NOTIFICATION LAWS, updated Oct. 12, 2010, http://www.ncsl.org/default.aspx?tabid=13489 (last visited Jan. 27, 2011) (providing access to all state security breach notification laws); MINTZ LEVIN, STATE DATA SECURITY BREACH LAWS, updated Sept. 1, 2010, http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (last visited Jan. 27, 2011) (providing analysis of each state data security law in chart form).

Take California as an example. Unlike on the federal level, California expressly recognizes a right to privacy in Article I, Section I of the state Constitution.[20] While the California Supreme Court refers to federal privacy decisions in interpreting that provision, it has recognized that the privacy protections in California are stronger than those at the federal level. Therefore, a federal preemption provision would directly weaken consumer protections currently in place, especially in states like California.

10. The Administration should review the Electronic Communications Privacy Act (ECPA), with a view to addressing privacy protection in cloud computing and location-based services. A goal of this effort should be to ensure that, as technology and market conditions change, ECPA continues to appropriately protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.

a. The Task Force seeks case studies and statistics that provide evidence of concern—or comments explaining why concerns are unwarranted—about cloud computing data privacy and security in the commercial context. We also seek data that link any such concerns to decisions to adopt, or refrain from adopting, cloud computing services.

Privacy Rights Clearinghouse agrees with the general statements above in 10. For data that address concerns with cloud computing data privacy and security in the commercial context, PRC refers the Department of Commerce to the 2010 report of the task force on Consumer Protection in Cloud Computing Services of the Consumer Federation of America.[21] We recommend this document as a resource for the Department.

We also recommend the 2009 cloud computing report by Robert Gellman, published by the World Privacy Forum.[22] Both of these reports discuss the unsettled legal environment for personal information held in the cloud.

When PRC communicates with individual consumers, we caution them about the risks of choosing to use the cloud, especially for sensitive personal information such as personal health records (PHRs).[23] We suggest that consumers download their records onto a personal computer hard drive rather than uploading them to the cloud until security and privacy issues are both better defined and resolved.

---

[20] Cal. Const. art. I § 1.

[21] CONSUMER FEDERATION OF AMERICA, CONSUMER PROTECTION IN CLOUD COMPUTING SERVICES: RECOMMENDATIONS FOR BEST PRACTICES FROM A CONSUMER FEDERATION OF AMERICA RETREAT ON CLOUD COMPUTING, Nov. 30, 2010, http://www.consumerfed.org/pdfs/Cloud-report-2010.pdf (last visited Jan. 27, 2011).

[22] WORLD PRIVACY FORUM. PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND SECURITY FROM CLOUD COMPUTING,. FEB. 23, 2009, HTTP://WWW.WORLDPRIVACYFORUM.ORG/PDF/WPF_CLOUD_PRIVACY_REPORT.PDF (LAST VISITED JAN. 28, 2011).

[23] *See* Privacy Rights Clearinghouse, *Online Personal Health Records: Are They Healthy for Your Privacy?*, revised March 2010, http://www.privacyrights.org/ar/Alert-PersonalHealthRecords-090421.htm (last visited Jan. 27, 2011).

b. The Task Force also seeks input on whether the current legal protections for transactional information and location information raise questions about what privacy expectations are reasonable and whether additional protections should be mandated by law. The Task Force also invites comments that discuss whether privacy protections for access to location information need clarification in order to facilitate the development, deployment and widespread adoption of new location-based services.

Privacy protections for access to location information do need clarification in order to facilitate the development, deployment and widespread adoption of new location-based services. Many consumers concerned about loss of privacy while using location-based services are unaware of who has access to their location-based information and how many different entities may have or subsequently gain access. In its publication titled "Location-Based Services: Time for a Privacy Check-In," the ACLU of Northern California states this well. "When many different companies hold copies of valuable information about consumers, the privacy protection afforded to consumers is only as strong as the weakest link."[24] Additional protections should be mandated by law, both to provide additional consumer protection, and to set norms to avoid uncertainty with regard to the development and implementation of emerging technologies.

Two primary issues that must be discussed are an individual's access to his or her personal location-based data, and when and whether law enforcement may access an individual's location-based data. For example, in 2010, while investigating bank robberies, the FBI demanded access to cell-phone records of every phone near each bank during the relevant robberies.[25] This is just one example of how law enforcement is using location data, and there are many others.[26] There must be clear standards for law enforcement use and acquisition of location-based data so that individuals know their rights and there is a lowered chance of law-enforcement abuse.

Because the judicial process is slow and individuals' rights to privacy are arguably being violated on a regular (if not daily) basis, the matter must be addressed through the legislative process. ECPA should address location-based data protections, and must be updated to reflect this.[27]

Commercial entities developing and profiting from location-based services and data have had the chance to protect consumers, and have not implemented measures to do so, either

---

[24] The ACLU of Northern California, *Location-Based Services: Time for a Privacy Check-In*, 2010, at 6, *available at* www.dotrights.org/lbs .

[25] Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET NEWS, Feb. 11, 2010, *available at* http://news.cnet.com/8301-13578_3-10451518-38.html .

[26] *See* ACLU, *supra* note 22.

[27] *See id*. at 11 (citing *ECPA Reform and the Revolution in Location-Based Technologies and Services, Hearing Before the Subcomm. On the Constitution, Civil Rights, and Civil Liberties of the H.H. Comm. on the Judiciary*, June 24, 2010).

through clear policies or choice mechanisms. Consumers must be able to make informed decisions surrounding the use of data associated with them.

In closing, we appreciate the opportunity to respond to the Department's privacy green paper.

Submitted by:

Meghan Bohn, Privacy Fellow

Beth Givens, Director
Privacy Rights Clearinghouse
3100 5th Ave., Suite B
San Diego, CA 92103
www.privacyrights.org