Comments of the Privacy Rights Clearinghouse

Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers

Preliminary FTC Staff Report

Federal Trade Commission

February 18, 2011

Table of Contents

I. Introduction

The Privacy Rights Clearinghouse (PRC) respectfully submits the following comments to the Federal Trade Commission for its consideration with respect to the December 2010 Preliminary FTC Staff Report: "Protecting Consumer Privacy in an Era of Rapid Change."

II. Background

The Privacy Rights Clearinghouse is a nonprofit organization, established in 1992 and located in San Diego, California. We have 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 reflect, in large part, 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.

III. General Statements

The Privacy Rights Clearinghouse appreciates the FTC's demonstrated effort to protect consumer rights in its Preliminary Staff Report: "Protecting Consumer Privacy in an Era of Rapid Change." It is increasingly important that consumers are given control over their own data, and that data is handled in a transparent manner.

Privacy Rights Clearinghouse is concerned by the fact that the framework proposed in the report is a self-regulatory strategy and does not address the possibility of enacting a comprehensive privacy law that incorporates Fair Information Principles (FIPs). While the report notes that FIPs form the basis of certain current privacy statutes, it does not acknowledge the importance of FIPs moving forward. Privacy Rights Clearinghouse advocates comprehensive baseline legislation that incorporates FIPs, such as the OECD Privacy Guidelines.[2]

To date, no meaningful online data privacy protections have resulted from industry self regulation. For this reason we are skeptical that self regulation will ever rise to the challenges of protecting privacy in an age of massive data collection, often conducted without the awareness and consent of individuals. However, we are encouraged by a recent statement by Commissioner

---

[1] *See* PRIVACY RIGHTS CLEARINGHOUSE, FACT SHEETS, http://www.privacyrights.org/Privacy-Rights-Fact-Sheets (last visited Feb. 10, 2011).

[2] Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[hereinafter OECD Privacy Guidelines], *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

Julie Brill that the FTC will seek Congressional action if industry does not act soon.[3] This was made in the context of Do Not Track.

When issuing the final report, we urge the FTC to adopt benchmarks moving forward to measure progress. At some defined point in time, the FTC must be able to move beyond self regulation if industry does not fully and effectively implement the privacy framework.

Following are the PRC's responses to questions presented in the FTC's Preliminary Report.

IV. Scope

Are there practical considerations that support excluding certain types of companies or businesses from the framework—for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?

The framework proposed in the FTC staff report is an important step forward in protecting consumer privacy. As the report recognizes, rapid technological advancements in our society give consumers access to better products and services but often at the cost of disclosing personal information. Often consumers are unaware of what personal data they are sharing, whether it is combined with other data, who they are sharing it with, how the data is subsequently handled and/or what risks are involved. In fact, "invisibility" is a key theme of the FTC report and is mentioned several times.

While some companies have embraced the self-regulation-based "notice-and-choice model" in good faith, this method of protecting consumer privacy interests has led largely to the creation of privacy policies not only lengthy and dense with legalese and technical jargon, but also often difficult to find and compare with other privacy policies. Other entities, notably in the data broker industry, do little to nothing to inform consumers or provide them with choices regarding the collection, handling or disposition of their data.

We are pleased that the proposed framework covers both online and offline data collection. The report states that "[t]he proposed framework would apply broadly to online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device" rather than restricting the framework to those who collect PII.[4] Based on the testimony and comments submitted to the FTC during its 2009-2010 roundtable process, the FTC is keenly aware of the ease with which data can be linked to consumers, computers and devices.

---

[3] Joe Mullin, *FTC Commissioner: If Companies Don't Protect Privacy, We'll Go to Congress*, PAIDCONTENT.ORG, Feb. 9, 2011, http://paidcontent.org/article/419-ftc-commissioner-if-companies-dont-protect-privacy-well-go-to-congress/ (last visited Feb. 15, 2011).

[4] FTC, Preliminary Staff Report: *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Dec. 2010, Introduction at v [hereinafter FTC Preliminary Staff Report], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

To address the above question, we believe the framework should be fully inclusive. It is necessary that companies handling consumer data conduct their business under general uniform standards. A broad scope for the framework promotes transparency and consumer awareness of data practices, and will, if implemented effectively and comprehensively, better allow for a baseline of privacy protection and informed consent.

V. Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services

A. Incorporate substantive privacy protections

Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?

The report lists these protections in Section V(B)(1):

- reasonable security safeguards
- collecting only information needed to fulfill a specific legitimate business need
- implementing reasonable data retention periods
- taking reasonable steps to ensure the accuracy of the data.

PRC recommends additional protections provided in both OECD's Privacy Guidelines and Canada's FIPs, codified in its national data protection law. For example, the principle of "use limitation" is not addressed in the FTC's framework. The principle addresses the fact that except by authority of the law or consent of the individual, "[p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those specified" at the time of data collection.[5] Use limitation fits well with the practice of collecting only information needed to fulfill a specific legitimate business need, but does need to be explicitly stated.

Any framework should also explicitly state that companies are accountable for their policies, practices and systems in compliance with any substantive protections. Accountability is a key FIP, one that should be addressed in section V(B)(1) of the final report.

In terms of balancing costs and benefits, we urge these to be weighed with the high expense of data breaches in mind. Privacy and security consultant Larry Ponemon estimates the cost per compromised record of a data breach to be $204.[6] But, there is more to measuring privacy protection than dollars and cents. Privacy consultant Robert Gellman discusses the costs to consumers and to society of *not* protecting privacy in a paper that describes how business

---

[5] *See* OECD Privacy Guidelines *supra* note 2, Part Two; Personal Information Protection and Electronic Documents Act, 2000, c.5 (Can.), *available at* http://laws.justice.gc.ca/en/showdoc/cs/P-8.6/sc:1/en#anchorsc:1 (see Schedule 1, Section 5, Principles).

[6] *See* Tom Field, *Cost of a Data Breach – Dr. Larry Ponemon, Ponemon Institute*, BANK INFO SECURITY, Feb. 2, 2010, http://www.bankinfosecurity.com/articles.php?art_id=2146 (last visited Feb. 15, 2011).

analyses are often biased.[7] In our comments we also discuss the very real human cost of the lack of personal privacy in a later discussion of data brokers.

B. Maintain comprehensive data management procedures

How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?

Privacy Rights Clearinghouse cannot emphasize enough the importance of adopting and maintaining comprehensive data management practices. On our website, we maintain a chronological list of data breaches from 2005 to the present. Although the compilation is by no means comprehensive, it currently lists 2,348 public data breaches, with the approximate number of records breached totaling 514,362,806.[8] The ever-growing chronology illustrates, however, that the "public shaming" strategy is not an effective incentive to the adoption of privacy-enhancing technologies.

The implementation of the privacy-enhancing technology of encryption would have prevented such data breaches, and the sensitive financial data of tens of millions of individuals would not have been put at risk.

Although the proposed framework will be an important catalyst in the adoption of PETs and in improving privacy protection practices in general, we believe the adoption of comprehensive baseline legislation that includes a private right of action will be far more effective. The continuation and expansion of FTC actions will also serve as a strong incentive for companies to develop and deploy PETs.[9]

VI. Companies should simplify consumer choice

A. Commonly accepted practices

Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?

The report states that companies would not be required to seek consent for certain commonly accepted practices: product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing.[10]

---

[7] Robert Gellman, *Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, Mar. 2002, http://epic.org/reports/dmfprivacy.pdf (last visited Feb. 15, 2011).

[8] CHRONOLOGY OF DATA BREACHES: SECURITY OF BREACHES 2005-PRESENT, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach#CP (last visited Feb. 14, 2011).

[9] Examples of such high-profile data security cases by the FTC include DSW Shoe Warehouse, BJ's Wholesale Club, and Card Systems. FTC Preliminary Staff Report, *supra* note 4, at 47 footnote 120.

[10] *See* FTC Preliminary Staff Report, *supra* note 4 at 53–54.

Fraud prevention is listed as a proposed commonly accepted practice, and the PRC recommends that the FTC consider dropping it from the list. If fraud prevention is ultimately listed as a commonly accepted practice for which companies do not need to provide choice to collect and use consumer data, it should be very clearly defined and subsequently monitored.

Including fraud prevention as a commonly accepted practice could be used as a loophole for companies to compile information, store it and eventually use it for other purposes. For example, in the early 2000s the practice of bars swiping the magnetic stripes of drivers' licenses to verify a patron's valid identification and age became a common practice. But some captured the data from the magnetic stripe and created their own databases for marketing purposes, precipitating legislation in California and other states.[11]

The commonly accepted practice of legal compliance is another that could be subject to abuse. This proposed exception should be written in a manner that does not encourage entities merely to store information just because someday law enforcement may need it.

Lastly, if first-party marketing is considered a commonly accepted practice it too will need to be narrowly defined to avoid confusion and abuse. There is considerable potential for individuals to be confused by this exception. Consumer expectations come into play here. We believe many individuals do not expect personal information to be shared with companies beyond the one they are dealing with. And most individuals do not read privacy policies where they would indeed learn just how far and wide their personal information is likely to be shared and sold. In fact, according to a study by the UC-Berkeley Samuelson Law, Technology and Public Policy Clinic, individuals were found to assume that a website will not share their personal information when they see the term "privacy policy."[12] PRC suggests that the FTC either omit first-party marketing as a commonly accepted practice, or very carefully and narrowly define the term and the practice.

Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing?

The short answer is "yes." Privacy Rights Clearinghouse believes that consumers should be given a choice before any personal data is used for marketing regardless of whether it is considered first- or third-party marketing, but this is especially critical for sensitive information.

---

[11] *See e.g.* Jennifer Lee, *Welcome to the Database Lounge*, N.Y. TIMES, Mar. 21, 2002, *available at* http://www.nytimes.com/2002/03/21/technology/welcome-to-the-database-lounge.html?src=pm.

The California law lays out the purposes for which a business may swipe a driver's license or identification card, and makes any violation a misdemeanor. CAL. CIV. CODE § 1798.90.1.

[12] *See* Chris Jay Hoofnagle & Jennifer King, *What Californians Understand about Privacy Online*, Sept. 3, 2008, http://ssrn.com/abstract=1262130 (last visited Feb. 15, 2011); Joseph Turow, Chris Jay Hoofnagle, et al., *The FTC and Consumer Privacy in the Coming Decade*, Nov. 8, 2006, http://www.law.berkeley.edu/files/FTC_Consumer_Privacy.pdf (last visited Feb. 15, 2011).

As we have stated elsewhere, consumers should have as much control as possible over what is done with their personal information.

Should first-party marketing be limited to the context in which the data is collected from the consumer?

If first-party marketing is ultimately considered a commonly accepted practice, it should be as narrowly defined as possible to avoid significantly stripping consumers of any right to control the use of their data. Furthermore, consumers should have the opportunity to accept or decline solicitations delivered through means other than those associated with the context in which the data is collected.

How should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both online and offline, to enrich its databases? Should companies provide choice about this practice?

Companies should be transparent regarding practices of data "enhancement," and indeed provide the opportunity for consumer consent. Because data "enhancement" processes are essentially invisible to consumers, the framework should emphasize affirmative consent to ensure both transparency and consumer control.

A case in point: on February 10, 2011, the Supreme Court of California held in *Pineda* v. *Williams-Sonoma* that a ZIP code constitutes personally identifiable information and therefore merchants may not ask customers using credit-cards for their ZIP codes.[13] This was primarily due to the fact that the company used a customer's ZIP in conjunction with her name to determine her address, which could then have been used for the retailer's own marketing purposes or to be sold to other businesses. The merchant used a data append process in violation of California law, the Song-Beverly Consumer Protection Act.[14]

B. Practices that require meaningful choice

General

What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category?

The most appropriate way to obtain consent from a consumer-oriented perspective is to provide an explicit opt-in mechanism. The consent must also be obtained in a manner that does not deceive or confuse consumers.

[13] Pineda v. Williams-Sonoma Stores, Inc., No. S178241 (Cal. Feb., 10, 2011).

[14] Song-Beverly Consumer Protection Act, CAL. CIV. CODE § 1747.08.

What types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services?

Privacy Rights Clearinghouse supports the just-in-time approach to disclosure and consent. Notices that are displayed at or near the time an individual makes a decision or is about to disclose personal information can take many forms as long as relevant information is not buried in a lengthy and jargon-laden privacy policy. The model GLB form offers a good example.[15] The most important information is displayed in a simple table with minimum verbiage. Such a format also enables individuals to engage in apples-to-apples comparisons with the policies of other companies. We discuss user friendly formats in section VIII.

What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide?

In our comments about companies that do not directly interact with consumers, we focus on the data broker industry.

The major source of personal information compiled and sold by data brokers is public records. Some companies are adding information from social media sites into the mix. Data brokers in turn provide or sell the information they collect to any number of entities depending upon their business models and how they monetize data. Purchasers of such data include law enforcement, media, employers, background screening companies, private investigators, skip tracers, attorneys and the general public. Some data brokers require that those purchasing data prove their legitimate business purpose. Others will sell to anyone. Unfortunately, some have been found to sell the information to identity thieves and insurers, for example.[16] And based on complaints we have received from individuals, we are aware of stalkers also obtaining such data.

The PRC has long advocated that individuals be given more control and choice regarding data broker practices. As the FTC is aware, this is difficult because such companies may never interact with the consumers themselves in either the collection or sale of the information. The even greater difficulty lies with the fact that "data broker" and "information broker" are relatively loose terms. In order to monitor, implement standards, and enforce actions regarding data brokers, this industry must be defined.

We are aware of the following definitions of data broker from past federal and state legislation that was unsuccessful:

---

[15] *See* Final Model Privacy Form under the Gramm-Leach-Bliley Act, http://www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm_Rule.pdf (last visited Feb.16, 2011).

[16] *See* United States v. ChoicePoint, Inc., No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/stipfinaljudgement.pdf; Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, WALL ST. J., Nov. 19, 2010, *available at* http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.

In 2009 Senator Leahy introduced the Personal Data Privacy and Security Act which defined data brokers as "business entities which, for monetary fees or dues, regularly engage in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals to nonaffiliated third parties on an interstate basis."[17]

In 2009 Rep. Rush introduced the Data Accountability and Trust Act which defined "information brokers" as:

> [An 'information broker' is] a commercial entity (or its contractor or subcontractor) whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity in order to sell or provide access to such information to any nonaffiliated third party.
>
> [S]uch definition does not include a commercial entity to the extent that such entity processes information collected by or on behalf of and received from or on behalf of a nonaffiliated third party concerning individuals who are current or former customers or employees of such third party to enable such third party to provide benefits for its employees or transact business with its customers. [18]

In 2009, a New York Governor's Program Bill, put forth for consideration by the legislature but never introduced, defines "individual reference services provider (IRSP)" as:

> [IRSP] means any person, agent, business, entity, affiliate or subsidiary who primarily engages in the business of collecting, assembling, transmitting or maintaining sensitive personal information for the purpose of providing access to such information about individual data subjects to third parties for monetary compensation or other consideration. [IRSP] activities shall not include provision of information to the federal or state government or any political subdivision thereof. A person or entity that engages in [IRSP] activities shall be presumed to be primarily engaged in such practice if the revenue such person or entity derives from such practice represents more than twenty percent of such person's or entity's professional service-related revenue. [19]

The definition did not include government entities, consumer reporting agencies, media, private investigators, and labor unions.

In 2005, California Senate Bill 550 contained the following definition of "data broker":

---

[17] Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009), summary available at http://www.govtrack.us/congress/bill.xpd?bill=s111-1490&tab=summary.

[18] Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009), summary available at http://www.govtrack.us/congress/bill.xpd?bill=h111-2221&tab=summary.

[19] An Act to amend the general business law, in relation to the protection of sensitive personal information; NY Governor's Program Bill, 2009 Memorandum, Bill #26.

> 'Data broker' means any person other than a governmental entity that regularly engages in compiling or maintaining consumer data files used or expected to be used or collected in whole or in part for the purpose of providing consumer data files, or access to those files, to nonaffiliated third parties for monetary fees, dues, or on a cooperative nonprofit basis.[20]

Not included were financial institutions subject to the California Financial Code, credit bureaus, "covered entities," and Internet Service Providers.

Privacy Rights Clearinghouse includes the above definitions in our comments to illustrate past attempts at defining "data broker" and to highlight the difficulty of delineating a scope that is neither too over- nor under-inclusive.

The PRC advocates for a more transparent and regulated data broker industry, which is only possible if "data broker" is clearly and thoughtfully defined. Later in the comments we make further suggestions regarding the data broker industry. We would support legislation to regulate this industry similar in some respects to the FCRA, giving individuals the rights of access, correction, and notice regarding adverse decisions. This recommendation is discussed in more detail in section VIII.B.

Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

Privacy Rights Clearinghouse recommends a mechanism whereby information brokers must register with a clearinghouse or registry created and monitored by the FTC.[21]

It should be noted that the PRC provides a list of more than 100 data brokers on our website; however, this list is not complete.[22] Some data brokers offer an opt-out to individuals. Some have even charged a fee to opt out.[23] As we discuss further below, consumers must be able to gain access to the information that is compiled about them and that may be used to influence decisions that may impact their lives.[24]

---

[20] California Data Broker Access and Accuracy Act of 2005, S.B. 550 (Cal. 2005), *available at* http://leginfo.public.ca.gov/pub/05-06/bill/sen/sb_0501-0550/sb_550_bill_20050628_amended_asm.pdf (version amended in assembly June 28, 2005).

[21] FTC Roundtable Series 1 on: Exploring Privacy, Matter No. P095416, Dec. 7, 2009, at 259(detailing statements made by Pam Dixon, Executive Director, World Privacy Forum, regarding data brokers and a proposed registry), *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf.

[22] ONLINE DATA VENDORS: HOW CONSUMERS CAN OPT OUT OF DIRECTORY SERVICES AND OTHER INFORMATION BROKERS, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/online-information-brokers-list (last visited Feb. 14, 2011).

[23] See the FTC's USSearch settlement, Online Data Broker Settles FTC Charges Privacy Pledges Were Deceptive, http://www.ftc.gov/opa/2010/09/ussearch.shtm (last visited Feb. 16, 2011)

[24] *See generally* Testimony of Pam Dixon, Before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy

VII. Special choice for online behavioral advertising: Do Not Track

Privacy Rights Clearinghouse strongly supports the creation and enactment of a universal Do Not Track mechanism to help consumers protect their online privacy. In its "What They Know" series, the *Wall Street Journal* states that "one of the fastest-growing businesses on the Internet is the business of spying on consumers."[25] Consumers often do not even know when their actions are being tracked, and many are concerned when they learn about these practices. Non-transparent data collection may also subject consumers to medical and financial targeting for instance, and differential pricing based on a profile.

How should a universal choice mechanism be designed for consumers to control online behavioral advertising?

Consumers must have the option to control the use of their personal data through a well-publicized, understandable and simple mechanism. This would ideally be achieved through a universal opt-in mechanism.

FTC Commissioner Julie Brill listed the following five criteria for such a mechanism at the Browser Privacy Mechanisms Roundtable,[26] hosted by the UC-Berkeley Center for Law and Technology on February 9, 2011:

- How easy the mechanism is to use.
- How effective and enforceable the mechanism is.
- Universality of the mechanism.
- Does the mechanism provide for opt-in or opt-out of collection and use?
- Are choices persistent?

Privacy Rights Clearinghouse would add that effectiveness of any Do Not Track mechanism for consumers should also be measured by a consumer's ability to set preferences down to the granular level if he or she so wishes.

The three major browsers have each developed their own strategies regarding Do Not Track in the context of online behavioral advertising.

Mozilla Firefox

---

and Commerce, *The Modern Permanent Record and Consumer Impacts from the Offline and Online Collection of Consumer Information*, Nov. 19, 2009, *available at* http://www.worldprivacyforum.org/pdf/TestimonyofPamDixonfs.pdf.

[25] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[26] For more general information on the Browser Privacy Mechanisms Roundtable see http://www.law.berkeley.edu/10219.htm (last visited Feb. 16, 2011).

Mozilla's approach centers on users being able to set a browser preference that will enable them to express the desire to opt out of third-party tracking. This is accomplished by transmitting a Do Not Track HTTP header to the site or page a user visits.[27] A Do Not Track header would not physically prevent tracking, but it would convey the request to the website that the consumer is visiting. Mozilla states, "We believe the header-based approach has the potential to be better for the web in the long run because it is a clearer and more universal opt-out mechanism than cookies or blacklists."[28]

The challenge lies in the fact that the website itself must honor the header request and would need to convey the request to any third parties that collect behavioral data from the site. To engender comprehensive adoption, the PRC believes that this would need to be addressed through legislation.[29] Nonetheless, if consumers begin using Mozilla's Do Not Track mechanism in Firefox,[30] or any similar header if adopted by other browsers, any data collected regarding site compliance with the request could facilitate the creation of "a paper trail of user intent, [and] it could allow a regulatory body to investigate claims of improper data usage."[31]

Microsoft Internet Explorer 9

Internet Explorer 9 (IE9) offers a feature called "Tracking Protection" which, when enabled by users, will help them control and block third-party tracking by creating or adding Tracking Protections Lists (TPLs). While IE9 accommodates TPLs and allows users to create them, Microsoft itself will not provide them.[32] When a user adds or creates a TPL, he or she may begin blocking ads, "third-party cookies, tracking pixels, web beacons, hit counters, analytics scripts, and other tools of the modern web designed to assemble a profile of your movements and activities on the web."[33]

---

[27] *See e.g.* Do Not Track, http://donottrack.us (last visited Feb. 7, 2011).

[28] First Person Cookie, More Choice and Control Over Online Tracking, Jan. 23, 2011, http://firstpersoncookie.wordpress.com/2011/01/23/more-choice-and-control-over-online-tracking/ (last visited Feb. 15, 2011).

[29] See e.g. Do Not Track Me Online Act of 2011, H.R.654, 112th Cong. (2011), *available at* http://speier.house.gov/uploads/Do%20Not%20Track%20Me%20Online%20Act.pdf for an example of a bill recently introduced in the House of Representatives by Congressperson Jackie Speier of California.

[30] *See id*.

[31] Mike Hanson, Thoughts on Do-Not-Track, open-mike.org, Jan. 23, 2011, http://www.open-mike.org/entry/thoughts-on-do-not-track (last visited Feb. 8, 2011).
"If a firm was found to track users in spite of the presence of affirmative Do-Not-Track headers, and after a reasonable length of time for implementation had elapsed, a stronger case could be made that they were infringing their user's privacy." *Id*.

[32] Update: Effectively Protecting Consumers from Online Tracking, IEBlog, Jan. 25 2011, http://blogs.msdn.com/b/ie/archive/2011/01/25/update-effectively-protecting-consumers-from-online-tracking.aspx#comments (last visited Jan. 25, 2011).

[33] Ed Bott, *IE9 and Tracking Protection: Microsoft disrupts the online ad business,* ZDNet, Feb. 13, 2011, http://www.zdnet.com/blog/bott/ie9-and-tracking-protection-microsoft-disrupts-the-online-ad-business/3004 (last visited Feb. 15, 2011).

An advantage of the list approach is that it is a more immediate solution for consumers than a header that will not likely be universally honored without legislative action. The list approach also gives consumers the ability to tailor their preferences in a granular manner. One downside to lists is that they must be maintained and may need to be updated frequently to remain effective.[34]

Google Chrome

Google Chrome offers a feature called "Keep My Opt-Outs," which allows users to "opt out permanently from ad tracking cookies."[35] Chrome's feature has been criticized because of its reliance on the NAI model. "All Google's highly touted add-on does is permanently keep your NAI cookie-based 'opt-out' options permanently in the browser."[36] "It also doesn't fix the other fundamental problems with the NAI's approach: complexity, the lack of a clear signal that can be observed and interpreted by *any* website, and allowing fake opt-outs that only protect you from targeted advertising but don't prevent any tracking."[37]

Overview of Options

We see clear benefits in both the header and list approach. In the short-term, consumers need a mechanism they can personalize to help them opt out of online behavioral advertising, and IE9 will provide that for individuals who use the IE9 browser. As a sustainable long-term solution, PRC advocates an enforceable header approach that will send a persistent message to sites when users do not want to be tracked, the Mozilla Firefox mechanism.

How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers?

Regardless of the form a Do Not Track mechanism takes, it must be user-friendly. Consumers should not need to search through multiple drop-down menus to find the mechanism. If the mechanism is browser-based or offered for use with a particular browser, the company should publish tutorials in the form of videos, animations, and/or diagrams in multiple languages that are easy to access. The educational resources surrounding the mechanism must also clearly spell out any limitations of the mechanism.

---

[34] *See* Hanson, *supra* note 31.

[35] Sean Harvey & Rajas Moonka, *Keep your opt-outs*, GOOGLE PUBLIC POLICY BLOG, Jan. 24, 2011, http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html (last visited Feb. 15, 2011).

[36] John M. Simpson, *Google's DNT Function is Deceptive*, CONSUMER WATCHDOG'S INSIDE GOOGLE, Feb. 1, 2011, http://insidegoogle.com/2011/02/google-dnt-function-is-deceptive/ (last visited Feb. 15, 2011).

[37] Rainey Reitman, *Mozilla Leads the Way on Do Not Track*, ELECTRONIC FRONTIER FOUNDATION DEEPLINKS BLOG, Jan. 24, 2011, http://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track (last visited Feb. 15, 2011).

What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?

Privacy Rights Clearinghouse acknowledges that there will likely be some effect on online publishers, advertisers, and those who have created a business model based on data generated through tracking. PRC does not believe that widespread use of a Do Not Track mechanism means the end of the free Internet as we know it, as industry spokespersons lament. Many tools already exist and are used by consumers to block all advertisements, not just ads based on behavioral tracking.

Further, behavioral advertising "accounted for, at most, just 4% of 2009 U.S. online advertising expenditures,"[38] and "projections place behavioral advertising at only 7% of the U.S. online advertising market in 2014."[39] Do Not Track would not affect contextual advertising, demographic advertising, search advertising, placement advertising, or even social network advertising.[40]

But let us not fail to look at the bigger picture. What is the impact on e-commerce if consumers do not trust the digital marketplace? Individuals must trust the web if they are to fully engage in e-commerce. If individuals do not feel they are being treated fairly when they visit commercial websites, e-commerce will not develop to its greatest capacity.

In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them?

A Do Not Track mechanism does not have to be an all-or-nothing proposition. It should be interactive and allow consumers to selectively allow tracking if and when they want. Most importantly, any mechanism should enable consumers to make timely informed decisions about the effects of allowing or disallowing tracking.

If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?

---

[38] Jonathan Mayer, *Do Not Track is No Threat to Ad-Supported Businesses*, The Center for Internet and Society, Stanford Law School, Jan. 20, 2011, http://cyberlaw.stanford.edu/node/6592 (last visited Feb. 4, 2011) (referencing Memorandum To: Members of the Subcommittee on Commerce, Trade, and Consumer Protection, From: Subcommittee on Commerce, Trade, and Consumer Protection Democratic Staff Re: Hearing on "Do Not Track Legislation: Is Now the Right Time?", Nov. 30, 2010, *available at* http://democrats.energycommerce.house.gov/documents/20101201/Briefing.Memo.12.01.2010.pdf).

[39] *Id.*

[40] *Id.*

To date, the private sector has not voluntarily implemented an effective universal choice mechanism.[41] The National Advertising Initiative has offered an opt-out cookie for online profiling since 2000, but it is not effective due in large part to the fact that many consumers do not know it exists, there is no requirement that companies engaging in online tracking participate, and there is no oversight or enforcement.[42]

In 2009, the Direct Marketing Association and industry association partners released Self-Regulatory Principles for Online Behavioral Advertising.[43] Not until January 2011, and almost certainly spurred by the FTC Preliminary Staff Report, did the DMA announce that it was "beginning enforcement activities to ensure industry compliance with the Principles."[44] The problems with voluntary principles, as illustrated by the NAI endeavor, include incomplete participation, lack of oversight and lack of enforcement.

We encourage the FTC to establish clear benchmarks for a successful implementation of a self regulatory approach to a uniform choice mechanism, both in how such a mechanism would function, as well as a timeframe for implementation. Given the failed history of self regulation over the decades, we believe legislation is the only option for meaningful and comprehensive consumer protection regarding online behavioral advertising and online tracking.

VIII. Companies should increase the transparency of their data practices

A. Improved privacy notices

What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

Privacy Rights Clearinghouse believes that it would not only be feasible, but also exceedingly beneficial to consumers to standardize the format and terminology for describing data practices within and across industries, particularly with respect to online and mobile privacy policies. Studies show that standardized privacy policy formats improve individuals' ability to find

---

[41]The FTC report acknowledges on page 64 that "industry efforts to implement choice on a widespread basis have fallen short. The FTC has been calling on industry to implement innovations such as 'just-in-time' choice for behavioral advertising since 2008." FTC Preliminary Staff Report, *supra* note 4.

[42] *See* Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, WORLD PRIVACY FORUM, Nov. 2, 2007, *available at* http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

[43] Direct Marketing Association, DMA and Key Trade Groups Release Comprehensive Privacy Principles for Use and Collection of Behavioral Data in Online Advertising, July 2, 2009, *available at* http://www.the-dma.org/cgi/dispannouncements?article=1308.

[44] *See* Direct Marketing Association, DMA Launches Enforcement for Online Behavioral Advertising (Jan. 31, 2011), http://www.the-dma.org/cgi/dispannouncements?article=1524 (last visited Feb. 16, 2011)

information and quickly make decisions.[45] As the FTC report notes, allowing consumers to make privacy-based decisions may also have the positive effect of driving marketplace competition on privacy issues.

Specifically, PRC advocates that the FTC follow a similar approach to that which was recently applied to financial institutions covered by the Gramm-Leach-Bliley Act with respect to the model form privacy notice and Online Form Builder.[46] We believe that a comparable form builder approach would provide consumers with consistent layout and terminology that would be easier to understand and compare in making informed personal privacy-based decisions.[47]

How can companies present these notices effectively in the offline world or on mobile and similar devices?

In the offline retail context, PRC suggests enacting a double opt-in system for consumers who are asked to share certain personal data. The system would require retail outlets to first inform and ask the consumer in person, and then confirm via e-mail or postal mail. Confirmation text should include the policy to which the consumer is agreeing and ideally require an opt-in mechanism (such as clicking through to the website to confirm creation of a user profile, calling a number, or sending a pre-paid postal notice back to the company).

For mobile devices, we recommend the development of standardized icons that visually impart information on data collection and privacy practices in a layered approach. Users would visit a website for additional information.

B. Reasonable access to consumer data

Should companies be able to charge a reasonable cost for certain types of access?

The issue of whether companies should be able to charge for certain types of access is a difficult one that merits more discussion than it is given in the FTC report. Sometimes information that is not stored in electronic format may be expensive to access, and may merit a reasonable cost based on the cost to access it and make it available to the consumer. Nonetheless, a consumer

---

[45] *See e.g.* P. Kelley, L. Cesce, J. Bresee, & L. Cranor, *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, CMU-CyLab-09-014, Carnegie Mellon University, Jan. 2010, *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf.

[46] *See generally*, Joint Press Release, Board of Governors of the Federal Reserve, Commodity Futures Trading Commission, Federal Deposit Insurance Company, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Securities and Exchange Commission, Federal Regulators Release Model Consumer Privacy Notice Online Form Builder, Apr. 15, 2010, *available at* http://www.federalreserve.gov/newsevents/press/bcreg/20100415a.htm.

[47] *See e.g.* FTC, Legal Resources, http://business.ftc.gov/legal-resources/46/36 (for resources regarding the model form builder and model forms). *See also* Final Model Privacy Form under the Gramm-Leach-Bliley Act, http://www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm_Rule.pdf. For a sample policy see Macy's Credit Card Privacy Policy, *available at* https://www.macys.com/service/credit/popups/privacy.jsp (Rev.10/10)(last visited Feb. 16, 2011).

should have access to his or her data, and should not be subjected to costs that prevent them from knowing what information an entity has regarding that individual.

Another scenario to consider, and potentially analogize with the question at hand, is that individuals used to have to pay for their credit reports. Under the Fair and Accurate Credit Transaction Act of 2003,[48] individuals can now obtain free annual credit reports. Regarding non-consumer facing companies, specifically data brokers, individuals should similarly be able to obtain access to the information held about them once a year at no charge, and be charged a reasonable fee thereafter. We discuss the challenge of authentication below within the context of data brokers. Because of this issue's complexities, we recommend that the FTC facilitate an in-depth discussion about fees in a workshop, suggested in our comments below.

Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?

Companies should inform individual consumers of the identity of those with whom the company has shared the consumer's data, and inform them of the source of that data. As the FTC notes on page 48 of the report, this is especially important because erroneous information from data brokers can be used to deny consumers access to funds, admission to an event, or membership in a group.

Where critical life decisions are made about individuals based on data files containing personal information, it is especially important that individuals know the identity of who has received that data as well as the source of the data. In the context of credit reporting and employment screening, the FCRA contains such provisions. Being able to correct erroneous data is just one reason it is important that individuals be able to follow the data trail.

The PRC has been contacted by a number of individuals who have had difficulty correcting data held about them by data brokers. It is virtually impossible for individuals to contact all data brokers, much less to determine where those data brokers obtained the information about them. We have learned that much of the data from public records that is obtained and sold by data brokers is provided by just a few data compilers. When we have inquired of data broker representatives about the identities of those few providers, we have been told that it is proprietary information.

Individuals who must correct information that is being propagated about them by data brokers are usually told that they must make those corrections at the "source," such as the court system. Unfortunately, that is not always an effective solution. When such individuals are being disadvantaged in, say, the job market by erroneous information supplied to employers and screening companies, time is of the essence. The employer's acquisition of incorrect data often leads to failure in one's job search.

We recommend that the FTC hold a workshop to delve into such matters regarding data brokers vis-à-vis unfair and deceptive business practices in order to develop systemic solutions. The

[48] Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.

FTC's complaints database, Sentinel, is likely to contain a significant number of complaints from individuals about the data broker industry and would be a good starting point to examine the practices of this industry.

Should access to data differ for consumer-facing and non-consumer-facing entities?

Consumers should be able to access data regardless of whether the entity is consumer-facing or non-consumer facing. With regard to non-consumer facing entities such as information brokers, the manner in which consumers are able to access data may realistically need to be different from the manner in which consumers access data from consumer-facing entities.

A key challenge regarding access to one's data held by non-consumer facing entities like data brokers is authentication of the requester. The company that holds that data must be sure it is providing access to the actual data subject and not to someone who is intent on fraud or, in the case of domestic violence and stalking victims, one who would violate the personal safety of the individual. While it is necessary to obtain sufficient information from the individual seeking access, the data broker must then not use that information to supplement its own database with information that it does not already have.

In 2005, the California Legislature considered a bill to give individuals a right of access to data broker files, Senate Bill 550 (introduced by then state Senator Jackie Speier). Although the bill failed, the FTC might find the documentation associated with the bill to be useful in its deliberation of this issue.[49]

As a side note, PRC would urge the FTC to reconsider or further define its statement that "the extent of access should be proportionate to the sensitivity of the data and the nature of its use."[50] Data sensitivity often depends on the individual to whom the data corresponds, and it is PRC's view that any data can be sensitive depending on the situation.[51]

For non-consumer-facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data?

As previously discussed, before there will be any transparency in the information broker industry, the members of that industry must be defined and identified. Privacy Rights Clearinghouse believes that the existence of a clearinghouse where brokers register and are listed on a site available to the public is the best way to allow consumers to seek access to their data and determine who possesses it. Consumers would benefit from knowing the name of the

---

[49] The text of the bill, legislative history, committee proceedings, and final disposition can be found at the official website of the California Legislature, http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_550&sess=0506&house=B&author=speier (last visited Feb. 16, 2011).

[50] FTC Preliminary Staff Report, *supra* note 4 at 72.

[51] *See* Beth Givens, *Comments Submitted to the Federal Trade Commission for Consideration in the Third Privacy Roundtable, Privacy Rights Clearinghouse*, Mar. 5, 2010, *available at* http://www.privacyrights.org/Third-Privacy-Roundtable-Comments-Submitted-to-Federal-Trade-Commission.

broker, the types of data it collects, and contact information or relevant data access information.[52]

We would also recommend a one-stop opt-out process. Today, some data brokers provide an opt-out opportunity to individuals, while others do not. The PRC has received numerous complaints from individuals who want to be able to opt out of their personal information being shared by all data brokers without having to go down the [incomplete] list of companies on the PRC website to determine which offer removal and which do not. Further, many data brokers erect barriers, whether intentionally or not, to opting out by requiring individuals to provide copies of personal documents such as the driver's license, to be mailed or faxed. Such authentication requirements vary from company to company and should be standardized and simplified.

Privacy Rights Clearinghouse has compiled a list of more than 100 online data brokers, and solicits input from the general public and data brokers to keep the list up-to-date.[53] We realize, however, that the list is not complete. It is an imperfect substitute to a mandated clearinghouse of data brokers.

Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?

We believe it is. First, the data broker industry must be defined and the players identified. This will not happen through self regulation, as the failed Individual Reference Services Group (IRSG) endeavor of the late 1990s illustrated. Legislation is needed to regulate the data broker industry with the codification of a robust set of FIPs, similar in many respects to the regulation of the credit reporting agencies under the FCRA.

In a self-regulatory environment, the problem lies in the fact that there is no way to ensure total participation. Even if participation were high among data brokers, this model would require frequent audits of the participating brokers to ensure compliance with the voluntary standards regarding the provision of access. We do not believe that is realistic.

Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?

Consumers should be entitled to receive notice when data about them has been used to deny benefits. However, "benefits" must be defined in order for this to be possible. It may be reasonable to use the Fair Credit Reporting Act (FCRA) as a model. The FCRA defines

---

[52] *See* FTC Roundtable Series 1 on: Exploring Privacy, Matter No. P095416, Dec. 7, 2009, at 259(detailing statements made by Pam Dixon, Executive Director, World Privacy Forum, regarding data brokers and a proposed registry), *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf.

[53] *See* ONLINE DATA VENDORS: HOW CONSUMERS CAN OPT OUT OF DIRECTORY SERVICES AND OTHER INFORMATION BROKERS, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/online-information-brokers-list (last visited Feb. 14, 2011).

"adverse actions" and states that after taking an adverse action based upon certain information in certain contexts, the consumer is entitled to notice.[54]

PRC is in strong agreement with the statement on page 76 of the FTC report that enacting such a notice requirement should allow consumers the benefit of an opportunity to contact information brokers and correct any false data upon which any such denial was based.

The notice should be provided in a format acceptable to the consumer. If appropriate and feasible, consumers should be able to specify the manner in which they would prefer to receive notice when they are informed that data about them will be used as a determining factor in being denied a "benefit" (however defined). In the event that the consumer does not specify a preferred medium through which to receive notice, there should be a default or back-up form of notice through postal mail.

The FCRA requires such notice and can be used as a model (both in the positive sense and the negative) in deliberating on the best way to provide such notice. Although employment background screening is not a topic of the FTC's report, it is an area of much concern to jobseekers, as evidenced by the numerous questions and complaints the PRC has received on this issue. In fact, problems and questions with employment background checks is consistently in the "top five" consumer issues on the PRC's phone and email hotline.

Based on our discussions with many individuals over the years, we believe there is considerable noncompliance with the notice requirement when an employer has made an adverse decision about a job applicant. The PRC filed comments with the FTC regarding this and other issues involving employment screening as part of the agency's privacy roundtable process.[55]

Senator Leahy's 2009 data broker bill contains a provision requiring notice when an adverse decision is made based on data broker information.[56]

> (1) IN GENERAL.—In addition to any other rights established under this Act, if a person takes any adverse action with respect to any individual that is based, in whole or in part, on any information contained in a personal electronic record that is maintained, updated, or otherwise owned or possessed by a data broker, such person, at no cost to the affected individual, shall provide—(A) written or electronic notice of the adverse action to the individual; (B) to the individual, in writing or electronically, the name, address, and telephone number of the data broker that furnished the information to the person; (C) a copy of the information such person obtained from the data broker; and (D) information to the individual on the procedures for correcting any inaccuracies in such information.

---

[54] *See generally* The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681, *et seq*., available at http://www.ftc.gov/os/statutes/fcradoc.pdf.

[55] Beth Givens, *Employment Background Checks: Observations of Erroneous Data and Noncompliance*, PRIVACY RIGHTS CLEARINGHOUSE, Apr. 14, 2010, http://www.privacyrights.org/employment-background-checks-observations (last visited Feb. 16, 2011).

[56] *See* Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s1490rs.txt.pdf.

(2) ACCEPTED METHODS OF NOTICE.—A person shall be in compliance with the notice requirements under paragraph (1) if such person provides written or electronic notice in the same manner and using the same methods as are required under section 313(1) of this Act.

This section of the FTC report further asks "What are the costs and benefits of providing such notice?" We are not able to speak to the actual dollar costs of providing such notice. But we can certainly discuss the human costs to individuals who do not receive such notices. Again, in the context of employment screening where we believe there is considerable noncompliance with the FCRA regarding adverse action notice, jobseekers are robbed of the opportunity to correct erroneous information that is impeding their job search. There is reputation damage as well. The employer may be left with the impression that the individual has, say, a criminal record, when in fact, it may be another "John Smith" whose criminal record was obtained in the screening process. Long-term unemployment is a likely result of such errors going uncorrected. Certainly, those costs are considerable, not only to the affected individuals, but to society.

In the context of the use of information obtained from a data broker to make an adverse decision about an individual, we can certainly extrapolate from what we have learned from jobseekers and apply it to the data broker industry. The human and societal costs of individuals not being notified of adverse decisions based on erroneous or outdated information are significant.

C. Material changes

What is the appropriate level of transparency and consent for prospective changes to data-handling practices?

Companies falling within the framework should implement the highest level of transparency and consent when enacting changes to data-handling practices. Privacy Rights Clearinghouse believes that consumers must be presented with the changes and then be given the opportunity to consent or opt-in to enact the changes.

Companies should be required to follow a stricter set of principles with respect to the following changes in data-handling practices: changing from an opt-in to an opt-out, changing from receiving access to receiving no access, changing from a free service to a fee service, changing a data retention period, and sharing or selling any information that the entity previously was not sharing or selling.

D. Consumer education

How can individual businesses, industry associations, consumer groups and government do a better job of informing consumers about privacy?

We focus our comments on businesses and on government, and for the latter, specifically the FTC.

First, businesses should implement visible and clearly worded privacy policies and notices. From the Privacy Rights Clearinghouse's perspective, this would be best achieved through the use of simplified and standardized forms created through a form-builder (as discussed above).

Businesses, especially those that are customer facing, should also increase their customer-service presence. It should be easy for a consumer to speak with a "live" representative if he or she chooses. A frequent complaint that we receive from individuals is the inability to talk in real time with a customer service agent, and as a result, the inability to resolve a problem or have a question answered.

In the online environment, businesses should also employ more "just-in-time" mechanisms for individuals as a way to inform them of their impending choice, as we have discussed above.

We laud the FTC for its extensive and rich website containing a wealth of information and tips for individuals. Its identity theft microsite is a particularly valuable resource for individuals and victims alike.[57] We recommend that the FTC create microsites on other topics of critical concern to individuals such as data brokers and employment screening.

Our country is extraordinarily diverse. It is important for businesses, industry associations, consumer groups, and government agencies to maximize the effectiveness of their educational messages by providing them in multiple languages. We also recommend that such messages be provided in formats other than text, such as videos that include animations and simple diagrams.

Ideally, the reading level for written materials should be at the 6th grade reading level, although that can be difficult to achieve. For an example of privacy-related educational materials that are written at the 6th grade level, see those provided by the California Office of Privacy Protection.[58]

We further recommend that usability testing be employed in the design of websites to ensure that educational resources are designed for maximum effectiveness.

IX. Conclusion

In closing, we express our sincere appreciation to the FTC for embarking on the ambitious process of convening the privacy roundtables, inviting expert and consumer input, releasing the preliminary staff report *Protecting Consumer Privacy in an Era of Rapid Change*, and undertaking the challenge of analyzing the hundreds of comments it is expected to receive in order to release its privacy framework by the end of the year. Please do not hesitate to contact us if you wish further information or clarification on any of the points we have raised.

Beth Givens, Director

---

[57] *See* FTC, Fighting Back Against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/ (last visited January 13, 2011).

[58] See privacy guides of the California Office of Privacy Protection available at http://www.privacy.ca.gov/consumers.htm (last visited Feb. 14, 2011). Note that guides are provided in languages other than English.

Meghan Bohn, Staff Attorney

Privacy Rights Clearinghouse
3100 5th Ave.
San Diego, CA 92103
Web: www.privacyrights.org