WORLD **PRIVACY** FORUM

Testimony of Pam Dixon Executive Director, World Privacy Forum

Before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce

What's a Consumer to Do? Consumer Perceptions and Expectations of Privacy Online

October 13, 2011

Chairman Mack, and Members of the Committee, thank you for the opportunity to testify today about consumers' expectations and perceptions of privacy online. My name is Pam Dixon, and I am the Executive Director of the World Privacy Forum. The World Privacy Forum is a 501(c)(3) non-partisan public interest research group based in California. Our funding is from foundation grants, cy pres awards, and individual donations. We focus on conducting in-depth research on emerging and contemporary privacy issues as well as on consumer education.

I have been conducting privacy-related research for more than ten years, first as a Research Fellow at the Denver University School of Law's Privacy Foundation where I researched privacy in the workplace and employment environment, as well as technology-related privacy issues such as online privacy. While a Fellow, I wrote the first longitudinal research study benchmarking data flows in employment online and offline, and how those flows impacted consumers.

After founding the World Privacy Forum, I wrote numerous privacy studies and commented on regulatory proposals impacting privacy as well as creating useful, practical education materials for consumers on a variety of privacy topics. In 2005 I discovered previously undocumented consumer harms related to identity theft in the medical sector. I coined a termed for this activity: medical identity theft. In 2006 I published a groundbreaking report introducing and documenting the topic of medical identity theft, and the report remains the definitive work in the area. In 2007 I coined and introduced the original Do Not Track idea. In 2010 I published the first report on privacy and digital signage networks.

Beyond my research work, I have published widely, including a 2011 reference book on online privacy (*Online Privacy*, ABC-CLIO) and seven books on technology issues with Random House, Peterson's and other large publishers, as well as more than one hundred

articles in newspapers, journals, and magazines.[1]

Today I will discuss consumer expectations of privacy online and the tremendous misperceptions and concomitant risks that exist for consumers. I will also discuss the features of past and current approaches that have allowed these problems to proliferate, with suggestions for remedies.

Online privacy is not just a theoretical exercise of academics and experts talking about potential risks that may someday occur. Privacy difficulties in the online world now readily leak over into the offline world with real consequences such as price discrimination, difficulty finding employment, problems with insurability, and sometimes just plain old embarrassment or social difficulties such as the loss of a friend. In some situations, misperceptions about what online privacy does and doesn't mean can lead to issues with personal finances, safety, and other aspects of well-being. As we documented in our 2010 report on digital signage, consumers' online activities now intersect with everyday activities in profound ways, including issues relating to facial recognition and identifiability.

I have observed that the regulatory conversation about what to do about online privacy often focuses on advertising, in particular behavioral advertising. This focus began in earnest in 1997 with the inception of the self-regulatory Network Advertising Initiative. The conversation continues today with a similar focus. There is an emphasis on self-regulatory efforts, and an emphasis on a narrow slice of privacy-related problems online.

We need to expand our privacy vocabulary and our thinking at this point. Online privacy includes advertising *and* it includes many other things now, including many other kinds of privacy risks from third parties. Online privacy risks include information leakage in many forms and varieties, and online privacy risks may be tied to offline behavior. Consumers simply do not know about these risks for the most part, and given the complexity of the online environment and the number and variety of privacy risks, I am not persuaded that consumer education can do enough quickly enough to be a viable stand-alone solution. I am also concerned that history indicates strongly that the current self-regulatory regimes will fail to adequately protect consumers from the privacy realities online.

In 2007 the World Privacy Forum held a meeting in Berkeley, California about online privacy. Our purpose was to find a collaborative way to have a broader, more accurate discussion about online privacy and to foster ideas about solutions to the existing problems that consumers face. We invited all of the leading privacy and consumer groups to the meeting. Most came. At that meeting, I proposed the Do Not Track idea, and I later wrote the original Do Not Track proposal collaboratively with the groups at the meeting

[1] Much of my privacy-related research work and writings are available at the World Privacy Forum web site, <http://www.worldprivacyforum.org>.

and submitted it to the FTC with signatories.[2] My idea behind Do Not Track was to provide consumers a way to opt out of the various forms of online and potentially offline tracking in one place. The idea was born from the knowledge of how deep the consumer misperceptions of online privacy protections are, and from the knowledge of just how challenging it is for consumers to truly manage their information online knowledgeably.

The World Privacy Forum believes that an approach that repeats the mistakes of past unsuccessful privacy protection efforts will replicate the same results. There needs to be a different approach. Later in this testimony, I will discuss potential ways forward in providing consumers with solutions to online privacy challenges. First, I would like to discuss the deep consumer misperceptions about online privacy that exist.

I. Consumer Expectations of Privacy: Deep Misperceptions About What is Happening Online and what is Protected … or Not

Consumers' expectations of privacy online rarely match the reality of what is happening to their information. Consumers don't have the ability to see or understand the information that is being collected about them,[3] and they don't have the tools to see how that information is impacting the opportunities that are being offered – or denied – to them. Consumers also believe incorrectly that privacy icons and privacy policies offer more protection for them than they actually do.[4] This disconnect is due to an abundance of consumer misperceptions of what privacy really means as defined by actual industry practices today. It is also due to the reality that it is extremely challenging for individual consumers to have the skills and knowledge to fully understand the information privacy risks they can encounter online, much less navigate the risks.

We see this first hand. The World Privacy Forum receives consumer queries about online privacy issues, and we have for years. The consumer complaints we have received run the gamut. We have received calls from surprised, worried, and frustrated consumers who discovered their private medical information online, consumers who wanted to figure out how to stop Google Street View from displaying images of their backyard, people who were not able to exercise opt outs at data broker web sites, consumers who were upset and privacy changes on Facebook, and many more. What the complaints have in common

---

[2] Do Not Track, *Consumer Rights and Protections In the Behavioral Advertising Sector*, October 30, 2007, *available at*: http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf.

[3] See, for example, a new Carnegie-Mellon study on one aspect of consumer data collection, behaviorally targeted online ads. This study found that "many participants have a poor understanding of how Internet advertising works, do not understand the use of first-party cookies, let alone third-party cookies, did not realize that behavioral advertising already takes place, believe that their actions online are completely anonymous unless they are logged into a website, and believe that there are legal protections that prohibit companies from sharing information they collect online." Aleecia M. McDonald and Lorrie Faith Cranor, Carneigie Mellon University, *An Empirical Study of How People Perceive Online Behavioral Advertising*, Nov. 10, 2009.

[4] Chris Jay Hoofnagle and Jennifer King, Samuelson Law, Technology and Public Policy Clinic, University of California-Berkeley School of Law, *What Californians Understand About Privacy Offline*, May 15, 2008.

was the question at the end of the conversation, which in many variations simply stated: what can I do?

I wish we had better answers for them. We often don't, because of the lack of consumer protections or rights in this core area of life for so many digital citizens. The consumers who contact us are those who *know* they have a privacy problem. They are the fortunate ones. Far more consumers are simply not aware of the risks they face.

Most consumers are not aware that based on their activities, online data handlers can build extensive profiles about consumers' backgrounds and interests. Third-party cookies from one company alone—Google—can track users' browsing activity across much of the web and collect data such as clickstream, ad impression history and ad click history.[5] A single click on a website can reveal plentiful information about a consumer – current location[6], parenthood, education, income range, shopping habits, and more.[7] Using this information obtained by tracking consumers, data handlers can construct detailed profiles[8] about the consumers.[9] These profiles are sometimes linked to individuals' identities.[10]

I want to emphasize that consumer tracking and targeting goes beyond web browsers. This will be an important area of inquiry going forward as online information access moves beyond traditional Internet connectors such as laptop computers. Data handlers track consumers when they connect to the Internet through a variety of devices such as mobile phones, televisions and video game consoles. When the device is a mobile phone, the tethering of consumers' habits to their device can be quite personal because consumers carry it all the time, and because advertisers have employed identifiers for tracking that are hard coded into the telephone. Unlike standard web cookies, these tracking tools lack controls and cannot be deleted. Applications and services on the

---

[5] A clickstream is a list of URLs visited by the user; an ad impression history is a list of ads that have been displayed to the user; an ad click history is a list of all ads that the user has clicked on. *See* Vincent Toubiana et al., *Adnostic: Privacy Preserving Targeted Advertising*, at 4; *see also* UC Berkeley, School of Information*, KnowPrivacy,* June 1st, 2009, http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf "Google in particular had extensive coverage. It had a web bug on 92 of the top 100 sites, and on 88% of the total domains reported in the data set of almost 400,000 unique domains."

[6] *Beyond Voice Mapping the Mobile Marketplace*, at 15-16, Federal Trade Commission Staff Report, (April 2009), *available at:* http://www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf. For example, when a consumer uses a location-based service — one of the widely used location-based applications is the mobile family and finder application that enables users to determine their family members' and friends' locations.

[7] Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, *available at:* http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html ("From a single click on a web site, [x+1] correctly identified Carrie Isaac as a young Colorado Springs parent who lives on about $50,000 a year, shop at Wal-Mart and rents kids' videos. The company deduced that Paul Boulifard, a Nashville architect, is childless, likes to travel and buys used cars. And [x+1] determined that Thomas Burney, a Colorado building contractor, is a skier with a college degree and looks like he has good credit.").

[8] A profile is a description of the user's interests inferred from the clickstream created by data handlers. *See* Vincent Toubiana et al., *Adnostic: Privacy Preserving Targeted Advertising*, at 4.

[9] Elli Androulaki & Steven Bellovin, *A Secure and Privacy-Preserving Targeted Ad-System*, at 1.

[10] Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL ST. J., October 25, 2010.

mobile phone allow data handlers to access consumers' current physical location using GPS technology.[11] For example, Apple's iPhone kept a record of real-time location information even when location services were turned off.[12] Although the location data is "anonymous," the data reveals a lot of information about the user such as home address, work location and daily routines. Because the information is so specific and personal, anyone who has access to it can potentially work out the identity of the user.[13] Therefore, the location information is not truly "anonymous" and poses significant privacy risk.

The information that has been collected online can be used to make snap judgments about consumers. This practice often shapes the consumer's online experience. Some financial companies show entirely different pages to visitors based on assumptions made about consumers' income and education level.[14] For example, credit card companies may present a set of high interest rate but easy-to-qualify credit card offers to a visitor based on the web-history-based assumptions that the visitor has a bad credit history. The visitor may in fact have a good credit score and may simply be interested in high-reward credit cards. To date, no court has applied fair-lending laws to the practice of using web-browsing history to make lending decisions. A bank could choose not to send a lending offer, or to send a different offer, based upon an applicant's browsing history, such as visits to a gambling site.[15]

There are further areas of consumer misperceptions about online privacy. We have highlighted just a few examples:

- Consumers who think they are visiting a single web page may be surprised to learn that if they registered at a site, some parts of their information, including in some cases email addresses and usernames, may be flowing to an invisible (to them) array of third parties, including advertisers. A Stanford study revealed that websites studied were leaking usernames and user IDs to third parties such as Facebook,ComScore, Google Advertising (Doubleclick), and Quantcast, among other parties. The study found that viewing a local ad on the Home Depot web site sent the user's first name and email address to 13 companies, among other data leakage examples.[16]

---

[11] Ashkan Soltani, *Testimony of Ashkan Soltani Before the Senate Committee on Commerce, Science, and Transportation Hearing on The State of Online Consumer Privacy*, March 16, 2011, at 4-5.
[12] Jennifer Valentino-Devries, *IPhone Stored Location in Test Even if Disabled*, WALL ST. J, April 25, 2011, *available at:* http://online.wsj.com/article/SB10001424052748704123204576283580249161342.html.
[13] Eric Chabrow, *Apple, Google Under Fire at Hearing*, Government Information Security, (May 10, 2011), *available at:* http://www.govinfosecurity.com/articles.php?art_id=3623
[14] 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.
[15] Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., (Aug. 4, 2010), *available at:* http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.
[16] Jonathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, Stanford Law School Center for Internet and Society, October 11, 2011, *available at:* http://cyberlaw.stanford.edu/.

Advertising companies incentivize consumers to identify themselves online by giving them free offers or requests for registration. Once the consumers identify themselves on a website, the historically tracked non-personally identifiable information can be merged with the personally identifiable information.[17] Unfortunately, this choice of "re-identification" is not always voluntary, as identifiable information can be leaked to third-party data handlers. For example, when a consumer makes purchase online, the merchant can share the consumer's email address, collected through the billing process, with a third party that was present on the purchase page.[18]

- A Wall Street Journal article revealed an online tracking company called RapLeaf collected information from social networking profiles and matched it with email addresses in order to link consumers' real world identities. In fact, RapLeaf admits that in addition to tracking consumers online, it also collected names and used the Facebook ID in compiling its database of consumer profiles. RapLeaf gathered and sold very specific information about individuals. The Journal uncovered that RapLeaf segmented people into more than 400 categories, such as income range, political leaning, religion, and interest in adult entertainment.[19]

- People who typed search queries to the AOL search bar had no idea that their search queries would be made public. In 2006, AOL released a compressed text file containing search keywords from users. Although AOL did not identify specific users in its report, individuals could still be identified and matched to their search history by the bits of disconnected personally identifiable information in the aggregated search queries. The New York Times was able to locate and interview an individual from the search records by cross-referencing the search data with publicly available phonebook listings.[20] If an individual can be identified using AOL search queries alone, companies or data handlers can similarly identify an individual by name using similar kinds of online behavioral information.

- Consumers may not realize that data handlers can gather information such as medical conditions, finances or sexual orientation indiscriminately. One Wall Street Journal article describes a high school graduate who often does online

---

[17] *Online Profiling: A Report to Congress*, at 4, Federal Trade Commission, (June 2000), *available at:* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf ("For example, a network advertising company could operate its own Web site at which consumers are asked to provide personal information. When consumers do so, their personal information could be linked to the identification number of the cookie placed on their computer by that company, thereby making all of the data collected through that cookie personally identifiable.").

[18] Ashkan Soltani, *Testimony of Ashkan Soltani Before the Senate Committee on Commerce, Science, and Transportation Hearing on The State of Online Consumer Privacy*, at 3-4, (March 16, 2011).

[19] Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL ST. J., (October 25, 2010).

[20] Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N. Y. TIMES, (August 9, 2006), *available at:* http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482.

research about weight loss.[21] The high school graduate sees weight-loss ads every time she goes on the Internet. "I'm self-conscious about my weight," she said. "I try not to think about it . . . Then the ads make me start thinking about it." There are technical steps this young woman could take to get rid of the ads, such as using the Mozilla web browser with an adblocking plug in. How many consumers know about such technologies? Did she?

II. Consumer Want Privacy Protection – But Misperceive Actual Protections

Consumers do want privacy protection. Surveys have indicated that people value privacy even when it is contrasted with other social or personal interests.[22] Most Americans do not want marketers to tailor advertisements to their interests.[23] Americans' rejection of even anonymous behavioral targeting indicates that they do not believe that the collected data will remain disconnected from their PII.[24] Research has unambiguously shown that consumers want to control and shape their online experience, and that they are worried about other uses of their data in ways they do not know or understand, and might not like.[25]

Consumers feel uneasy about online tracking. In 2000, a study found that 67% of individuals were "not at all comfortable" if a Website shared their information so they could be tracked on multiple Websites. The same study reveals that 63% of individuals were "not very comfortable" or "not at all comfortable" when a website tracked their movements when they browsed the site, even if those data are not tied to their names or real-world identities.

Another study in 2000 found that consumers would spend a total of $6 billion more per year online if they did not feel that their privacy was at stake every time they made a transaction online. A 2007 study found that consumers are willing to pay approximately 60 cents more per fifteen-dollar spent to protect their privacy online.

These consumer expectations are clear: consumers want online privacy. But the problem is that consumer expectations are not aligned correctly with what protections are available and what privacy indicators mean.

---

[21] 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.

[22] Priscilla Regan, *Legislating privacy: Technology, social values, and public policy*, at 177, Chapel Hill, U.S., The University of North Carolina Press.

[23] Joseph Turow et al., *Americans Reject Tailored Advertising*, at 3, (September 2009), *available at:* http://ssrn.com/abstract=1478214. 66% of adult Americans do not want marketers to tailor advertisements to their interests. When Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages, between 73% and 86%, say they would not want such advertising.

[24] Joseph Turow et al., *Americans Reject Tailored Advertising*, at 4, (September 2009), *available at:* http://ssrn.com/abstract=1478214.

[25] Joseph Turow et al., *Americans Reject Tailored Advertising*, at 4-5, (September 2009), *available at:* http://ssrn.com/abstract=1478214.

A groundbreaking 2008 study on what consumers understood about privacy online revealed that a majority of California consumers who see privacy policies on a web site overvalue the protections the privacy policy offers in multiple ways. For example, respondents believed that privacy policies create a right for deletion of data upon request. Online shoppers believed that online privacy policies prohibited third-party information sharing.[26] Additional studies have backed up these findings of consumers over-estimating privacy protections.[27]

Given the disparity between what is actually happening online and what consumers believe is protected, it is no surprise that consumers do not take affirmative action to protect themselves. Every person who uses the Internet is not necessarily technologically skilled or a privacy expert. Even with such expertise, the reality is that the solutions that are available to most consumers are limited.

III. Lessons from History: Correcting the Course of Consumer Protection

The World Privacy Forum supports consumer-protective legislation in the area of online privacy. We note that if self-regulation is going to be the course of action, it is absolutely critical to construct self-regulation differently than it has been done in the past. In 2007, the World Privacy Forum (WPF) issued a report on the National Advertising Initiative's early efforts at business-operated self-regulation for privacy. The report was *The NAI: Failing at Consumer Protection and at Self-Regulation*.[28] In 2010, the World Privacy Forum issued a report on privacy activities of the Department of Commerce, *The US Department of Commerce and International Privacy Activities: Indifference and Neglect*.[29] Tomorrow we will be publishing a new report on the history of privacy self-regulation, which we include in this testimony today. Next week, we are publishing a detailed analysis of the Digital Advertising Alliances' self-regulatory program, a report that we prepared in collaboration with the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley School of Law.

We can summarize what we have learned from our work. Privacy self-regulation in the past has been a Potemkin Village of privacy protection. The self-regulatory privacy programs appear when there is a threat of legislation, then they disappear when the eye of the regulatory storm passes by. The programs look good from a distance, but upon closer inspection they offer no substantive consumer privacy protections.

---

[26] Chris Jay Hoofnagle, Jennifer King, *What Californians Understand About Privacy Online*, September 3, 2008.
[27] *See* 2. *See also* Joseph Turow, *Americans and Online Privacy, The System is Broken*, Annenberg Public Policy Center (June 2003), *available at*: http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.
[28] http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (last visited 10/12/11).
[29] http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (last visited 10/12/11).

If privacy self-regulation is undertaken in the same way it has been in the past, history indicates those efforts will fail. Self-regulation created by industry, for industry, and then policed by industry has a very poor track record.

Consider these past industry self-regulatory privacy programs, of which only one is in existence today:

- The **Individual Reference Services Group** was announced in 1997 as a self-regulatory organization for companies providing information that identifies or locates individuals. The group terminated in 2001, deceptively citing a recently-passed regulatory law as making the group's self-regulation unnecessary. However, that law did not cover IRSG companies.

- The **Privacy Leadership Initiative** began in 2000 to promote self-regulation and to support privacy educational activities for business and for consumers. The organization lasted about two years.

- The **Online Privacy Alliance** began in 1998 with an interest in promoting industry self-regulation for privacy. OPA's last reported substantive activity appears to have taken place in 2001, although its website continues to exist and shows signs of an update in 2011, when FTC and congressional interest recurred. The group does not accept new members.[30]

- The **Network Advertising Initiative** had its origins in 1999, when the Federal Trade Commission showed interest in the privacy effects of online behavioral targeting. By 2003, when FTC interest in privacy regulation had diminished, the NAI had only two members. Enforcement and audit activity lapsed as well. NAI did not fulfill its promises or keep its standards up to date with current technology until 2008, when FTC interest increased.

- The **BBBOnline Privacy Program** began in 1998, with a substantive operation that included verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component. Several hundred companies participated in the early years, but interest did not continue and BBBOnline stopped accepting applications in 2007. The program has now disappeared.

The self-regulatory programs advanced by the industry can be thought of as quasi-contracts with consumers. Lawmakers permit the industry to continue its profitable enterprise of Online Consumer Tracking and Profiling without strict legal oversight and consumers are supposed to get a level of privacy in return. In today's terms, the sets of self-regulatory principles advanced for example by the Network Advertising Initiative

[30] http://www.privacyalliance.org/join/. (Last visited October 12, 2011.)

and the Digital Advertising Alliance are the terms. The analysis the World Privacy Forum has conducted indicates that the terms are lacking and consumers are not getting a fair bargain.

IV. Going Forward

In our report on the history of self-regulation, we discuss ideas for doing things differently, in a way that will work to correct the mistakes of the past. These ideas include:

- **Tension in the Process:** Successful privacy self-regulation requires standards responsive to the actual problems, robust policies, meaningful enforcement, and effective remedies. Privacy self-regulation of industry, by industry, and for industry will not succeed. Tension in self-regulation can be provided by a defined and permanent role for consumers who are the intended beneficiaries of privacy protection. Government may also be able to play a role, but government cannot be relied upon as the sole overseer of the process. The past has shown that the interest of the FTC waxed and waned with the political cycle, and the Department of Commerce did not provide sufficient oversight.

- **Scope:** The scope of a self-regulatory regime must be clearly defined at the start. It must apply to a reasonable segment of industry, and it must attract a reasonable percentage of the industry as participants. There must be a method to assess the penetration of the self-regulatory regime in the defined industry.

- **Fair Information Practices:** Any self-regulatory regime should be based on Fair Information Practices (FIPs). Implementation of FIPs will vary with the industry and circumstances, but all elements of FIPs should be addressed in some reasonable fashion.

- **Open Public Process:** The development of basic policies and enforcement methods should take place to a reasonable degree in a public process open to every relevant perspective. The process for development of privacy self-regulatory standards should have a reasonable degree of openness, and there should be a full opportunity for public comment before any material decisions become permanent. Consumers must be able to select their own representatives. Neither government nor those who are to be regulated should select consumer participants – the selection should be up to the consumers.

- **Independence:** The organization that operates a privacy self-regulatory system needs to have some independence from those who are subject to the self-regulation. Those who commit to comply with privacy self-regulation must make a public commitment to comply for a term of years and a financial commitment for that entire period.

- **Benchmarks:** Past self-regulatory efforts and codes of conduct lack benchmarks for success. What constitutes success? Is it membership? Market share? Is it actual enforcement of the program? Without specific benchmarks for a privacy program, it is much more difficult to gauge success in real-time. Without the ability to accurately assess activities within a current program, both success and failure are more difficult to ascertain and may only be gleaned in hindsight.

Another evaluative tool exists. The United Kingdom-based National Consumer Council ("NCC") published a checklist for self-regulatory schemes in 2000 that provides a starting point to discuss what the industry principles should contain.[31] The checklist provides the following requirement for a "credible" self-regulatory scheme:

1. The scheme must be able to command **public confidence**.

2. There must be strong **external consultation and involvement** with all relevant stakeholders in the design and operation of the scheme.

3. As far as practicable, the operation and control of the scheme should be **separate** from the institutions of the industry.

4. Consumer, public interest and other **independent representatives must be fully represented** (if possible, up to 75 per cent or more) on the governing bodies of self-regulatory schemes.

5. The scheme must be based on **clear and intelligible statements of principle** and **measurable standards** – usually in a Code – which address **real consumer concerns**. The objectives must be rooted in the reasons for intervention [].

6. The rules should **identify the intended outcomes**.

7. There must be clear, accessible and **well-publicised - complaints procedures** where breach of the code is alleged.

8. There must be adequate, meaningful and commercially significant **sanctions** for non-observance.

9. **Compliance must be monitored** (for example through complaints, research and compliance letters from chief executives).

10. **Performance indicators** must be developed, implemented and published to measure the scheme's effectiveness.

[31] *See* National Consumer Council, *Models of self-regulation: An overview of models in business and the professions* 51-52 (November 2000), *available at:* http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf.

11. There must be a degree of **public accountability**, such as an Annual Report.

12. The scheme must be **well publicised**, with maximum education and information directed at consumers and traders.

13. The scheme must have **adequate resources** and be funded in such a way that the objectives are not compromised.

14. **Independence** is vital in any redress scheme which includes the resolution of disputes between traders and consumers.

15. The scheme must be regularly reviewed and **updated** in light of changing circumstances and expectations.[32]

V. Conclusion

Consumers no longer have the option of simply living in an opt-out village[33] and avoiding going online to conduct the business of their daily lives. That is not a realistic choice anymore. Given the deep lack of understanding about the complexity and pervasiveness and impact of online privacy web leakage and tracking, consumers need practical options about how to handle their information privacy online and off. Consumer misperception about what and when privacy protective mechanisms are in force complicates matters further. If consumers knew the risks, they would have more opportunity to change behaviors. If consumers understood actual privacy protections, they may make different choices about information sharing.

Currently, no substantial protections are available for consumers. Most privacy self-regulatory schemes that have been produced thus far have many defects. The current online self-regulatory programs have many of the characteristics of past self-regulatory programs that eventually disappeared altogether. If Congress is to avoid a Potemkin Village of consumer protection, the path forward will need to include a very new and fresh approach to the issue of consumer protection.

We support legislation, but if faced with a situation where there is no legislation, then we urge Congress to look deeply at the flaws of past self-regulatory efforts and do things differently this time. We urge Congress to look at the deeper question facing online privacy today: what can we do differently that will give consumers a better result?

---

[32] National Consumer Council, *Models of self-regulation: An overview of models in business and the professions* 51-52 (November 2000), *available at* http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf (emphasis in original).

[33] The idea of the "Opt Out Village" arises from a video spoof on privacy published by the Onion. Google Opt Out Feature Lets Users Protect Privacy by Moving to Remote Village, The Onion, < http://www.theonion.com/video/google-opt-out-feature-lets-users-protect-privacy,14358/ >.

Thank you for your invitation to testify and your attention today.

Respectfully submitted,

Pam Dixon

Attachment:

Many Failures: A Brief History of Privacy Self-Regulation in the United States, Robert Gellman & Pam Dixon, World Privacy Forum, October 14, 2011.