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.

World Privacy Forum

Many Failures: A Brief History of Privacy Self-Regulation in the United States

Robert Gellman & Pam Dixon

October 14, 2011

Brief Summary of Report

Efforts to create self-regulatory, or voluntary, guidelines in the area of privacy began in 1997. Privacy self-regulation was promoted at the time as a solution to consumer privacy challenges. This report reviews the leading efforts of the first self-regulatory wave from 1997 to 2007, and includes a review of the life span, policies, and activities of the Individual Reference Services Group, Privacy Leadership Initiative, Online Privacy Alliance, Network Advertising Initiative, BBBOnline Privacy Program, US-EU Safe Harbor Framework, Children's Online Privacy Protection Act, and the Platform for Privacy Preferences. A key finding of this report is that the majority of the industry self-regulatory programs that were initiated failed in one or more substantive ways, for example, many have disappeared. The report concludes with a discussion of possible reforms for the process for example, a defined and permanent role for consumers, independence, setting benchmarks, and other safeguards.

About the Authors

Robert Gellman is a privacy and information policy consultant in Washington DC. (www.bobgellman.com.) Pam Dixon is the Executive Director of the World Privacy Forum. Gellman and Dixon are the authors of *Online Privacy A Reference Handbook* (ABC CLIO, 2011.)

About the World Privacy Forum

The World Privacy Forum is a non-profit consumer education and public interest research group. It focuses on a range of privacy matters, including financial, medical, employment and online privacy. The World Privacy Forum was founded in 2003. www.worldprivacyforum.org.

I. Introduction and Summary

Current online privacy debates focus on respecting the privacy interests of Internet users while accommodating business needs. Formal and informal proposals for improving consumer privacy offer different ideas for privacy *regulation* and privacy *self-regulation,* sometimes called *codes of conduct*.[34] Some in the Internet industry continue to advance or support ideas for privacy self-regulation. Many of these same players proposed and implemented privacy self-regulatory schemes that started in the late 1990s.

Missing from current debates on self-regulation in the online privacy arena is a basic awareness of what happened with the first round of industry self-regulation for privacy. Also missing are the lessons that that should have been learned from the failures of past privacy self-regulatory efforts.

This report reviews the history of the leading efforts that comprised that early wave of privacy self-regulation, which occurred from 1997 to about 2007. One purpose of this report is to document the facts about that first wave of self-regulation. The other purpose of this report is to inform current discussions about the recent past. A key finding of this report is that the majority of the industry self-regulatory organizations that were initiated have now disappeared. The disappearance of a self-regulatory organization constitutes a failure of the self-regulatory scheme.

This is not the first World Privacy Forum report on privacy self-regulation. 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*.[35] In 2010, the WPF issued a report on privacy activities of the Department of Commerce, *The US Department of Commerce and International Privacy Activities: Indifference and Neglect*.[36] The Commerce report reviewed in some detail the government supervised self-regulatory Safe Harbor Framework for personal data exported from Europe to the US. Unlike most other privacy self-regulatory efforts, the Safe Harbor Framework continues to exist, largely because of the government role. But the Safe Harbor Framework is deficient in enforcement and some other areas, and it cannot be counted as successful.

The privacy self-regulation programs reviewed in this report were effectively a Potemkin Village of privacy protection. Erected quickly, the schemes were designed to look good from a distance. Upon closer inspection, however, the protections

---

[34] This report uses *self-regulation* instead of the term *codes of conduct*.
[35] http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (last visited 9/20/11).
[36] http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (last visited 9/20/11).

offered were just a veneer. The privacy Potemkin Village fell down soon after the gaze of potential regulators drifted elsewhere. Efforts such as the Individual Reference Service Group (IRSG) and the National Advertising Initiative (NAI) are examples of classic, failed privacy self-regulatory efforts. These and other poorly designed privacy self-regulation schemes had limited market penetration and insufficient enforcement. Still, that was enough to fend off regulators until political winds blew in other directions.

Many participants to the debate are new to the issue and are unaware of recent history. Even the Federal Trade Commission has a short memory. The FTC appeared to acknowledge the limits of self-regulation when, it concluded in 2000 that self-regulatory programs fell "well short of the meaningful broad-based privacy protections the Commission was seeking and that consumers want."[37] But in 2010, a staff report from the FTC continued to show support for self-regulation as an alternative to legislation, seemingly ignoring the Commission's own experience from ten years earlier.[38] The pressure to believe that "this time, things will be different" remains significant. This belief is fueled by industry pressure, industry desire for no formal regulation, a continually shifting political environment, and the absence of meaningful rulemaking authority at the Federal Trade Commission.

This report offers a simple and clear history lesson. Industry self-regulation for privacy as it has been done in the past has failed. Past industry self-regulatory programs for privacy have lacked credibility, sincerity, and staying power. This report does not propose a new model for self-regulation, but it does conclude with some suggestions for a different approach that is based on a a defined role for consumers, more transparency, better definitions, and firmer commitments by those subject to self-regulation.[39]

---

[37] See Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report To Congress* 35 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited 9/20/11).

[38] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers* (Preliminary Staff Report 2010) at 66, http://ftc.gov/os/2010/12/101201privacyreport.pdf, (last visited 9/20/11) ("Such a universal [Do Not Track] mechanism could be accomplished by legislation or potentially through robust, enforceable self-regulation.")

[39] The National Consumer Council (UK) published a checklist for self-regulatory schemes in 2000 that remains worthy of attention. *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 (last visited 9/21/2011). The checklist offers the following requirements 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

It is beyond the scope of this report to consider whether the public's demands for greater privacy protections should be met with legislation, self-help mechanisms, some yet untested form of activity (regulatory, co-regulatory, or otherwise), or nothing at all.[40] This report is offered as a resource to help those who are debating these questions today.

Characteristics Common to Privacy Self-Regulation

This report reviews early industry self-regulatory activities for privacy during the years just before and after 2000. This period was the high watermark for privacy self-regulation. This report distinguishes between industry efforts at self-regulation, and government efforts. For most industry-supported self-regulatory efforts for privacy, a clear pattern developed in the years covered by this review. Feeling pressure from Federal Trade Commission scrutiny and from legislative interest, industry self-regulatory efforts for privacy developed quickly in an attempt to avoid any formal regulation. It can be observed that the self-regulatory activities typically were characterized by some or most of the following qualities:

- Self-regulatory organizations were most often based in Washington, D.C, where potential regulators are.
- Self-regulatory organizations formulated their rules in secret, typically with no input from non-industry stakeholders.
- The governing boards of privacy self-regulatory organizations typically had no non-industry board members of these groups. There were typically few or no consumer representatives.

---

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. 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.

[40] For a thoughtful discussion of self-regulation and analysis of alternatives, see Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S A Journal of Law and Policy for the Information Society 356 (2011), available at http://www.is-journal.org/hotworks/rubinstein.php (last visited 9/20/11).

- Privacy self-regulatory rules covered only a fraction of an industry or covered an industry subgroup, leaving many relevant business practices and many players untouched.

- Privacy self-regulation organizations were short-lived, typically surviving for a few years, and then diminishing or disappearing entirely when pressure faded.

- Privacy self-regulation organizations were loudly promoted despite their limited scope and substance.

- Privacy self-regulation organizations were structurally weak, lacking meaningful ability to enforce their own rules or maintain memberships. Those who subscribed to self-regulation were usually free to drop out at any time.

- Privacy self-regulation organizations were typically underfunded, and industry financial support in some cases appeared to dry up quickly. There was no long-term plan for survival or transition.

Not all of these characteristics were present in government supervised self-regulatory efforts, although those efforts were not necessarily any more successful.

Summary of Privacy Self-Regulatory History

Self-regulatory efforts do not fall neatly into narrow categories. However, some generalizations may be made that efforts fell into two broad categories, industry-supported and government-supported. One exception exists that is a mix of government, civil society, industry, and academia.

Industry-Supported Self-Regulatory Programs

The early **industry-supported** privacy self-regulatory efforts included:

• 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.[41]

• 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.[42]

• 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.

Government-Supported Self-Regulatory Efforts

Not all privacy self-regulatory efforts were solely industry supported. Some were government sponsored in some manner, and there is one effort that involved consumers, academics, public interest groups as well as industry. These efforts included:

• The **US-EU Safe Harbor Framework** began in 2000 to ease the export of data from Europe to US companies that self-certified compliance with specified Safe Harbor standards. Three studies have documented that compliance was spotty, with many and perhaps most companies claiming to be in the Safe Harbor not meeting the requirements. The Department of Commerce continues to run the program but has undertaken negligible oversight or enforcement. Thus, the Safe Harbor Framework is a form of government-supervised self-regulation but with little evidence of active supervision. Some EU data protection authorities recently rejected reliance on the Safe Harbor framework because of its lack of reliability.

• The **Children's Online Privacy Protection Act** (COPPA), which passed in 1998, involves both legislation and self-regulation. It is

---

[41] http://www.privacyalliance.org/join/. (Last visited October 12, 2011.)
[42] This report evaluates the original NAI self-regulatory program that existed until 2007/2008.

technically a form of government-supervised self-regulation. The COPPA law provides for a safe harbor provision[43] that is sometimes cited as a self-regulatory program. Industry participation in the COPPA safe harbor program is not widespread. Under COPPA, the same statutory standards apply whether a business is in the COPPA safe harbor program or not.

Combination Self-Regulatory Efforts

• The **Platform for Privacy Preferences Project** (P3P) is a standard for communicating the privacy policies of a website to those who use the website. A user can retrieve a standardized machine-readable privacy policy from a website and use the information to make a decision about how to interact with the website. Sponsors presented a prototype at an FTC Workshop in 1997, and the first formal technical specification came in 2000. Major web browsers still support P3P in part, and there is some usage by websites. A 2010 study found that there are widespread errors in implementation of P3P requirements and that large numbers of websites that use P3P compact policies are misrepresenting their privacy practices, misleading users and making the privacy protection tools ineffective.

This report does not aim to be comprehensive. We have limited the scope to the early, leading efforts. Some privacy self-regulatory efforts developed or revived more recently.[44] The Network Advertising Initiative began in 1999 and nearly disappeared a few years later. NAI revived around 2008, when FTC interest in online privacy reawakened, and industry felt threatened once again by regulation and legislation. This report discusses the early iteration of the NAI. The NAI issued a new set of self-regulatory principles in 2008, and membership increased. The revival of NAI follows the earlier pattern so far. Because the new NAI effort is still underway, this report does not attempt to evaluate the NAI's post-1998 efforts. The new NAI looks a lot like the old NAI, however. Also not reviewed in this report is TRUSTe.[45]

---

[43] 15 U.S.C. §§ 6501-6506.

[44] The Digital Advertising Alliance self-regulatory program is not analyzed in this report, as it was launched in July 2009 and falls out of range of this study. *See* http://www.aboutads.info (last visited 9/21/11).

[45] TRUSTe, a privacy seal that continues to exist, became a for-profit company in 2008. Saul Hansell, *Will the Profit Motive Undermine Trust in Truste*?, New York Times (July 15, 2008), http://bits.blogs.nytimes.com/2008/07/15/will-profit-motive-undermine-trust-in-truste (last visited 2/14/11). TRUSTe has morphed significantly in its scope, purpose, and composition during its lifetime, and as such requires a separate discussion. TRUSTe is discussed in this report in the context of the first iteration of the NAI program and in the context of P3P. For more on TRUSTe see also Ben Edelman, *Certifications and Site Trustworthiness* (Sept. 25, 2006), http://www.benedelman.org/news/092506-1.html (last visited 2/14/11) ("Of the

II. Discussion: Industry-Supported Self-Regulatory Programs for Privacy

This section offers a historical review of privacy self-regulation that occurred in the years just before and just after 2000. For a variety of reasons, it is not necessarily fully comprehensive. Some self-regulatory efforts may have disappeared without a trace. Activities within existing trade associations are difficult or impossible to assess from evidence available to those outside the associations. However, this discussion captures the leading organizations of the time. [46]

This review does not generally attempt to complete a comprehensive analysis of the quality of each self-regulatory effort. The standards promulgated by the self-regulatory programs were often general and quickly became outdated because of technology and other changes. It appears that audits or reviews of compliance with self-regulatory standards were often not attempted, not completed, not credible, or not transparent. Finding original documents is often difficult or impossible now. However, there is enough available information to describe the programs, their rise, their activities, and in some cases, their demise.

Individual Reference Services Group

The creation of the Individual Reference Services Group (IRSG) was announced in June 1997 at a workshop held by the Federal Trade Commission.[47] According to a document filed with the FTC, the group consisted of companies that offered individual reference services that provided information that identifies or locates

---

sites certified by TRUSTe, 5.4% are untrustworthy according to SiteAdvisor's data, compared with just 2.5% untrustworthy sites in the rest of the ISP's list. So TRUSTe-certified sites are more than twice as likely to be untrustworthy.”). See also the discussion of the Platform for Privacy Preferences (P3P) later in this document for a reference to numerous TRUSTe certified websites that had errors in implementation of P3P requirements.

[46] Also, privacy seal programs arose during the period of this review, but some disappeared entirely. None beyond BBBOnline and TRUSTe developed sufficient credibility, reliability, or public recognition to warrant investigation in this report.

[47] Federal Trade Commission, *Individual Reference Services, A Report to Congress* (1997), http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm (last visited 9/20/11).

individuals.[48] The IRSG reported fourteen "leading information industry companies" as members, including US Search.com, Acxiom, Equifax, Experian, Trans Union, and Lexis-Nexis.[49]

The IRSG described its self-regulatory activities in this manner:

> The core of the IRSG's self-regulatory effort is the self-imposed restriction on use and dissemination of non-public information about individuals in their personal (not business) capacity. In addition, IRSG members who supply non-public information to other individual reference services will provide such information only to companies that adopt or comply with the principles. The principles define the measures that IRSG members will take to protect against the misuse of this type of information. The restrictions on the use of non-public information are based on three possible types of distribution that the services provide.[50]

A principal purpose of the IRSG plan appeared to be to avoid any real regulation. It was successful in achieving that goal. In its 1999 report to Congress, the FTC recommended that the industry be left to regulate itself despite some *significant shortcomings*:

> A. Recommendations Regarding the IRSG Principles
>
> The Commission recommends that the IRSG Group be given the opportunity to demonstrate the viability of the IRSG Principles.
>
> The present challenge is to protect consumers from threats to their psychological, financial, and physical well-being while preserving the free flow of truthful information and other important benefits of individual reference services. The Commission commends the initiative and concern on the part of the industry members who drafted and agreed to the IRSG Principles, an innovative and far-reaching self-regulatory program. The Principles address most concerns associated with the increased availability of non-public information through individual reference services. With the promising compliance assurance program, the Principles should substantially lessen the risk that information made available through the services is misused, and should address consumers' concerns about the privacy of non-public information in the services' databases. Therefore, the Commission recommends that the IRSG Group be given the opportunity to demonstrate the viability of the IRSG Principles. ***

---

[48] Individual Reference Services Group, Industry Principles — Commentary (Dec. 15, 1997), http://www.ftc.gov/os/1997/12/irsappe.pdf (last visited 9/20/11).
[49] http://web.archive.org/web/19990125100333/http://www.irsg.org (last visited 9/20/11).
[50] Id.

> The Commission looks to industry members to determine whether errors in the transmission, transcription, or compilation of public records and other publicly available information are sufficiently infrequent as to warrant no further controls.
> While the Commission believes the IRSG Principles address most areas of concern, certain issues remain unresolved. Most notably, the Principles fail to provide individuals with a means to access the public records and other publicly available information that individual reference services maintain about them. Thus, individuals cannot determine whether their records reflect inaccuracies caused during the transmission, transcription, or compilation of such information. The Commission believes that this shortcoming may be significant, yet recognizes that the precise extent of these types of inaccuracies and associated harm has not been established. An objective analysis could help resolve this issue. The IRSG Group has acknowledged the Commission's position, and has demonstrated its awareness of this problem by (1) stating that it will seriously consider conducting a study of this issue and (2) agreeing to revisit the issue in eighteen months. The Commission looks to industry members to undertake the necessary measures to establish whether inaccuracies and associated harm resulting from errors in the transmission, transcription, or compilation of public records and other publicly available information are sufficiently infrequent as to warrant no further controls.[51]

One of the IRSG principles called for an annual "assurance review" for compliance with IRSG standards.[52] The IRSG also required that a summary of the report and any subsequent actions taken be publicly available. While the IRSG website contains some evidence that at least some IRSG members conducted reviews, the IRSG did not make the reports public on its website so it is not possible to determine whether the reviews were properly conducted, comprehensive, or otherwise meaningful.[53]

Once the threat of regulation evaporated or diminished, the IRSG continued in existence for a few years. In September 2001, approximately four years after it was

---

[51] Federal Trade Commission, *Individual Reference Services, A Report to Congress* (1997) (Commission Recommendations), http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm (last visited 9/20/11).

[52] http://web.archive.org/web/20020210151622/www.irsg.org/html/3rd_party_assessments.htm (last visited 9/20/11).

[53] See http://web.archive.org/web/20020215163015/www.irsg.org/html/irsg_assessment_letters--2000.htm (last visited 9/20/11). Whether the reports were made public in other ways has not been explored.

established, the IRSG announced its termination.[54] The stated reason was that legislation made the self-regulatory principles no longer necessary.

> "We are operating in a much different regulatory environment than we were when the IRSG was created in 1997," said Ron Plesser with Piper Marbury Rudnick & Wolfe LLP, whose firm represents the IRSG. "It doesn't make sense to maintain a self-regulatory program when this information is now regulated under the Gramm-Leach-Bliley Act."[55]

However, the legislation cited as the reason for termination (The Gramm-Leach-Bliley Act) *did not in fact regulate IRSG members*. The Gramm-Leach-Bliley (GLB) Act provided that each *financial institution* has an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[56] A financial institution is a company that offers financial products or services to individuals, like loans, financial or investment advice, or insurance.[57] The IRSG companies – companies that provide information that *identifies* or *locates* individuals – are not financial institutions under GLB. It is also noteworthy that GLB became law almost two years before it was cited as the reason for the end of the IRSG. GLB was a fig leaf that covered the lack of continuing industry support for the IRSG.

Why did the IRSG issue a deceptive statement about the reason for its termination? According to reports current at the time, the members of IRSG lost interest in supporting an expensive self-regulatory organization because they no longer felt threatened by legislation or regulatory activities.

The IRSG.org website is now owned by a link farm.[58]

The Privacy Leadership Initiative

A group of industry executives with members including IBM, Procter & Gamble, Ford, Compaq, and AT&T established the Privacy Leadership Initiative (PLI) in June

---

[54] http://web.archive.org/web/20020202103820/www.irsg.org/html/termination.htm (last visited 9/20/11).
[55] Id.
[56] 15 U.S.C. § 6801(a).
[57] 15 U.S.C. § 6809(3). See also Federal Trade Commission, *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act* (2002), http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act (last visited 9/20/11).
[58] See www.irsg.org (last visited 9/20/11).

2000.[59] PLI promptly began an ad campaign in national publications to promote industry self-regulation of online consumer privacy. According to a contemporary news account, the PLI initiative "follows a recent Federal Trade Commission recommendation that Congress establish legislation to protect online consumer privacy."[60]

A description of the PLI from its website in 2001 stated:

> The Privacy Leadership Initiative was formed by leaders of a number of different companies and associations who believe that individuals should have a say in how and when their personal information can be used to their benefit.
>
> The purpose of the PLI is to create a climate of trust which will accelerate acceptance of the Internet and the emerging Information Economy, both online and off-line, as a safe and secure marketplace. There, individuals can see the value they receive in return for sharing personally identifiable information and will understand the steps they can take to protect themselves. As a result of sharing, individuals will have the power to enhance the quality of their lives through personalized information, products and services.[61]

Another statement from the PLI website provides a more expansive statement of the origin and purpose of the organization:

> Why We Formed
>
> The PLI was formed to provide consumers with increased knowledge and resources to help them make informed choices about sharing their personal information. We also help businesses, both large and small — in all industries — develop and maintain good privacy practices. Trust and choice are the foundation of good privacy practices, yet research shows that there is currently a lack of trust between consumers and businesses. Individuals must trust responsible businesses to use personal information in ways that benefit them — such as better, less expensive and personalized products and services — while also providing them with choices about how much personal information is gathered and by whom. Through the establishment of a common understanding about the benefits

---

[59] See Marcia Savage, *New Industry Alliance Addresses Online Privacy*, Computer Reseller News (06/19/00), http://technews.acm.org/articles/2000-2/0621w.html#item13 (last visited 9/20/11).
[60] Id.
[61] http://web.archive.org/web/20010411210453/www.understandingprivacy.org/content/about/index.cfm (last visited 9/20/11).

> of exchanging personal information and how it can be safeguarded, the PLI will begin to restore consumer confidence.
>
> What We're Doing
>
> Given that privacy is a question of trust and behavior, the PLI is developing an "etiquette"--model practices for the exchange of personal information between businesses and consumers. We will help create this code of conduct by engaging in a multi-year, multi-level effort to educate consumers and businesses. Specifically, the PLI will:
> 1. Conduct original research to measure and track attitudes and behavior changes among consumers and to better understand how the flow of information affects the economy and people's lives on a day-to-day basis;
> 2. Compile and refine existing privacy guidelines and create The Privacy Manager's Resource Center, a new service for that assists businesses in developing their privacy programs
> 3. Design an interactive Web site — understandingprivacy.org — to make privacy simpler for consumers, businesses, trade groups, journalists, academics, policymakers and all other interested parties; and
> 4. Educate consumers about technology and tools that protect their interests without diminishing the benefits of exchanging personal preferences with responsible companies.
>
> Whether online or off, the flow of information is critical to the growth and success of our economy. Members of the PLI recognize that businesses must take an active role in ensuring that privacy practices evolve to meet consumer needs. While there is no simple answer for an issue this complex, for PLI members that means understanding what individuals want, tackling those challenges and initiating change, while being accountable and building confidence. These are the keys to creating a climate of trust between responsible businesses and consumers.[62]

Other accounts from the time support the notion that PLI was intended to promote self-regulation. A 2001 story on Internet privacy from a publication of the Wharton School at the University of Pennsylvania focused on the self-regulation goal:

> While Congress debates legislation on Capitol Hill, the business community is actively promoting other options. Chief among these is self-regulation.
>
> Earlier this month, for example, the Privacy Leadership Initiative (PLI) - a group of executives from such companies as AT&T, Dell Computer, Ford,

---

62 http://web.archive.org/web/20010419185921/www.understandingprivacy.org/content/about/fact.cfm (last visited 9/20/11).

> IBM and Procter & Gamble – announced a $30-$40 million campaign aimed at showing consumers how they can use technology to better protect their privacy online.[63]

By the middle of 2002, the threat of regulation has diminished enough so that PLI "transitioned" its activities to others. The BBBOnLine, a program of the Better Business Bureau system,[64] took over the PLI website (understandingprivacy.org). The BBBOnline privacy program, which lasted longer than the PLI, is no longer operational, and its details are discussed elsewhere in this paper.

By the middle of September 2002, the transition of the website to BBBOnLine appeared to be complete.[65] However, by January 2008, the understandingprivacy.org website had changed entirely, offering visitors an answer to the question *Can microwave popcorn cause lung disease?*[66] By the beginning of 2011, the understandingprivacy.org website was controlled by Media Insights, a creator of "content-rich Internet publications."[67] Other Media Insights websites include BunnyRabbits.org, Feathers.org and PetBirdReport.com.[68] It is an ignominious end point.

The Online Privacy Alliance

The Online Privacy Alliance[69] was created in 1998 by former Federal Trade Commissioner Christine Varney.[70] OPA's earliest available webpage described the

---

[63] *Up for Sale: How Best to Protect Privacy on the Internet*, Knowledge@Wharton (March 19, 2001), http://knowledge.wharton.upenn.edu/article.cfm?articleid=325 (last visited 9/20/11).

[64] Press Release, *Privacy Leadership Initiative Transfers Initiatives to Established Business Groups* (July 1, 2002), http://goliath.ecnext.com/coms2/gi_0199-1872940/Privacy-Leadership-Initiative-Transfers-Initiatives.html (last visited 9/20/11).

[65] http://web.archive.org/web/20020914095335/www.bbbonline.org/understandingprivacy (last visited 9/20/11).

[66] http://web.archive.org/web/20080118171946/http://www.understandingprivacy.org (last visited 9/20/11).

[67] http://www.mediainsights.com (last visited 9/20/11).

[68] Id.

[69] The main webpages for the organization are at www.privacyalliance.org. However, for a brief period starting in 2005, the Internet Archive shows that the organization also maintained webpages at www.privacyalliance.com. The first pages reported by the Internet Archive for www.privacyalliance.org are dated December 2, 1998.

organization as *a cross-industry coalition of more than 60 global corporations and associations*.[71]

The first paragraph of the background page on its website stated clearly its interest in promoting self-regulation:

> Businesses, consumers, reporters and policy makers at home and abroad are watching closely to see how well the private sector fulfills its commitment to create a credible system of self-regulation that protects privacy online. One of the most important signs that self-regulation works is the growing number of web sites posting privacy policies.[72]

In July 1998, OPA released a paper describing *Effective Enforcement of Self-regulation*.[73] In November 1999, a representative of the OPA appeared at an FTC workshop on online profiling and participated in a session on the role of self-regulation.[74] OPA self-regulatory principles were cited by industry representatives before the FTC and elsewhere.[75]

It is difficult to chart with precision the deterioration of the OPA. By all appearances, the OPA is defunct. It no longer accepts members, and the primary evidence of its activity is continuing small changes to their website. A review of webpages available at the Internet Archive shows a decline of original OPA activities starting in the early 2000s. For example, the first webpage available for 2004 prominently lists OPA news, but the first item shown is dated March 2002 and the next most recent item is dated November 2001.[76] The OPA news on the first webpage available for 2005 shows four press stories from 2004, but the most recent OPA item was still

---

[70] http://web.archive.org/web/19990209062744/www.privacyalliance.org/join/background.shtml (last visited 9/20/11).

[71] Id.

[72] http://web.archive.org/web/19990209062744/www.privacyalliance.org/join/background.shtml (last visited 2/8/11).

[73] http://web.archive.org/web/19981202200600/http://www.privacyalliance.org (last visited 9/20/11).

[74] http://www.ftc.gov/bcp/workshops/profiling/991108agenda.htm (last visited 9/20/11).

[75] See, e.g., Statement of Mark Uncapher, Vice President and Counsel, Information Technology Association of America, before the Federal Trade Commission Public Workshop on Online Profiling (October 18, 1999), http://www.ftc.gov/bcp/workshops/profiling/comments/uncapher.htm (last visited 9/20/11).

[76] http://web.archive.org/web/20040122052508/http://www.privacyalliance.org (last visited 9/20/11).

November 2001.[77] By 2008, The OPA news on the first webpage available for that year shows 2 news stories from 2006, and no reported OPA activity more recent than 2001.[78] There is little or no evidence after 2001 of OPA activities or participation at the Federal Trade Commission.[79] The threat that fostered the creation of the OPA apparently had disappeared. Wikipedia categorizes OPA under *defunct privacy organizations*.[80]

The OPA website continues to exist and appears to have been reformatted and updated at some time after 2008. The website has some links to recent new items, but a *More OPA News* link at the bottom connects to a webpage that shows no item more recent than 2001.[81] The main OPA webpage also includes links to old OPA documents such as *Guidelines for Online Privacy Policies* (approximately 533 words) and *Guidelines for Effective Enforcement of Self-Regulation* (approximately 1269 words). The website continues to offer old items, such as an OPA *Commentary to the Mission Statement and Guidelines* dated November 19, 1998.[82]

The list of members on its website as recently as May 2011 included at least one company (Cendant) that no longer existed at that time.[83] The membership page was not dated, and members number approximately 30, or less than half the number reported in 1998. The website now reports that membership is "closed".

The Network Advertising Initiative[84] (1999-2007 version)

The network advertising industry announced the formation of the Network Advertising Initiative at an FTC workshop in 1999. NAI issued its standards, a 21-

---

[77] http://web.archive.org/web/20050104085718/http://www.privacyalliance.org (last visited 9/20/11).
[78] http://web.archive.org/web/20080201111641/http://www.privacyalliance.org (last visited 9/20/11).
[79] www.ftc.gov (last visited 9/20/11)
[80] http://en.wikipedia.org/wiki/Online_Privacy_Alliance (last visited 9/20/11).
[81] http://www.privacyalliance.org/news (last visited 9/20/11).
[82] http://www.privacyalliance.org/news/12031998-4.shtml (last visited 9/20/11).
[83] http://web.archive.org/web/20110512024943/http://www.privacyalliance.org/members (last visited 9/20/11)
[84] This summary is adapted from a comprehensive review of the Network Advertising Initiative (NAI) published by the World Privacy Forum in 2007. The WPF report is THE NETWORK ADVERTISING INITIATIVE: Failing at Consumer Protection and at Self-Regulation. The WPF report contains citations and support for the conclusions presented here. http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (last visited 9/20/11).

page document, the next year.[85] The core concept – the opt-out cookie – has been criticized as a technical and policy failure, and it remains highly controversial.[86] The NAI is of particular note because the Federal Trade Commission voted on its creation.

When it began, NAI membership consisted of 12 companies, which was a fraction of the industry engaging in behavioral ad targeting. By 2002, membership hit a low of two companies.[87] This was a significant lack of participation by the industry. When the NAI created a category of associate members who were not required to be in full compliance with the NAI standards, membership increased, with associate members outnumbering regular members by 2006. Eventually, NAI eliminated the associate membership category.[88]

The NAI delegated enforcement of its standards to TRUSTe, an unusual action given that TRUSTe was a member of NAI for one year.[89] Over several years, the scope of TRUSTe public reporting on NAI complaints decreased consistently until 2006, when separate reporting about NAI by TRUSTe stopped altogether.[90] There is no evidence that the audits of NAI members that were required by NAI principles were conducted. No information about audits of members was ever made public.[91]

Much of the pressure that produced the NAI came from the Federal Trade Commission. Industry reacted in 1999 to an FTC behavioral advertising workshop, and the NAI self-regulatory principles were drafted with the support of the FTC.[92] Pressure from the FTC diminished or disappeared quickly, and by 2002, only two NAI members remained. When the FTC again showed interest in online behavioral advertising in 2008, the NAI began to take steps to fix the problems that had developed with its 2000 principles.[93] One of those steps was "promoting more robust self-regulation by today opening a 45-day public comment period concurrent with the release of a new draft 2008 NAI Principles."[94] NAI never sought public comment on the original principles.

---

[85] Id. at 7-8.
[86] Id. at 14-16.
[87] Id at 28-29.
[88] Id. at 29-30.
[89] Id. at 25.
[90] Id. at 33-36.
[91] Id. at 37.
[92] Id. at 9.
[93] See, e.g., Network Advertising Initiative, *Written Comments in Response to the Federal Trade Commission Staff's Proposed Behavioral Advertising Principles* (April 2008), http://www.ftc.gov/os/comments/behavioraladprinciples/080410nai.pdf (last visited 9/20/11).
[94] Id.

Because we remain in a period of renewed Federal Trade Commission and congressional interest in privacy, it is too soon to evaluate the new NAI efforts. Only when the pressure for better privacy rules has faded will it be possible to evaluate the new NAI activities fairly.

There were substantive problems with the original NAI principles as well. The conclusion of the World Privacy Forum Report summarizes the NAI failures:

> The NAI has failed. The agreement is foundationally flawed in its approach to what online means and in its choice of the opt-out cookie as a core feature. The NAI opt-out does not work consistently and fails to work at all far too often. Further, the opt-out is counter-intuitive, difficult to accomplish, easily deleted by consumers, and easily circumvented. The NAI opt-out was never a great idea, and time has shown both that consumers have not embraced it and that companies can easily evade its purpose. The original NAI agreement has increasingly limited applicability to today's tracking and identification techniques. Secret cache cookies, Flash cookies, cookie re-setting techniques, hidden UserData files, Silverlight cookies and other technologies and techniques can be used to circumvent the narrow confines of the NAI agreement. Some of these techniques, Flash cookies in particular, are in widespread use already. These persistent identifiers are not transparent to consumers. The very point of the NAI self-regulation was to make the invisible visible to consumers so there would be a fair balance between consumer interests and industry interests. NAI has not maintained transparency as promised.
>
> The behavioral targeting industry did not embrace its own self-regulation. At no time does it appear that a majority of behavioral targeters belong to NAI. For two years, the NAI had only two members. In 2007 with the scheduling of the FTC's new Town Hall meeting on the subject, several companies joined NAI or announced an intention to join. Basically, the industry appears interested in supporting or giving the appearance of supporting self-regulation only when alternatives are under consideration. Enforcement of the NAI has been similarly troubled. The organization tasked with enforcing the NAI was allowed to become a member of the NAI for one year. This decision reveals poor judgment on the part of the NAI and on the part of TRUSTe, the NAI enforcement organization. Further, the reporting of enforcement has been increasingly opaque as TRUSTe takes systematic steps away from transparent reporting on the NAI. If the enforcement of the NAI is neither independent nor transparent, then how can anyone determine if the NAI is an effective self-regulatory scheme? The result of all of these and other deficiencies is that the protections promised to consumers have not been realized. The NAI self-regulatory agreement has failed to meet the goals it has stated, and it

> has failed to meet the expectations and goals the FTC laid out for it. The NAI has failed to deliver on its promises to consumers.[95]

The NAI self-regulatory effort that began in 1999 was a demonstrable failure within a few years.

BBBOnline Privacy Program

The BBBOnline Privacy Program began in 1998, in response to "the need identified by the Clinton Administration and businesses for a major self-regulation initiative to protect consumer privacy on the Net and to respond to the European privacy initiatives."[96] Founding sponsors included leading businesses, such as AT&T, GTE, Hewlett-Packard, IBM, Procter & Gamble, Sony Electronics, Visa, and Xerox.[97] The program was operated by the Council of Better Business Bureaus through its subsidiary, BBBOnLine. There may have been some consumer group participation in the development of the BBBOnLine privacy program.

The BBBOnline Privacy Program was much more extensive than many other efforts at the time. It included "verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component."[98] To qualify, a company had to post a privacy notice telling consumers what personal information is being collected, how it will be used, choices they have in terms of use. Participants also had to verify security measures taken to protect their information, abide by their posted privacy policies, and agree to an independent verification by BBB*OnLine*. Companies had to participate in the programs' dispute resolution service,[99] a service that operated under a 17-page set of detailed procedures.[100] The dispute resolution service also reported publicly

---

[95] World Privacy Forum *NAI Report* at 39.

[96] New Release, Better Business Bureau, *BBBOnLine Privacy Program Created to Enhance User Trust on the Internet* (June 22, 1998), http://www.bbb.org/us/article/bbbonline-privacy-program-created-to-enhance-user-trust-on-the-internet-163 (last visited 2/10/11).

[97] Id.

[98] The earliest web presence for the BBB Online Privacy Program appeared at the end of 2000. http://web.archive.org/web/20010119180300/www.bbbonline.org/privacy (last visited 9/20/11).

[99] http://web.archive.org/web/20010201170700/http://www.bbbonline.org/privacy/how.asp (last visited 9/20/11).

[100] http://web.archive.org/web/20030407011013/www.bbbonline.org/privacy/dr.pdf (last visited 9/20/11).

statistics about its operations.[101] As noted above, the BBBOnLine Privacy Program took over the Privacy Leadership Initiative website (understandingprivacy.org) when PLI ended operations in 2002. The BBBOnline Privacy Program was considerably more robust than most, if not all, of the contemporary privacy-self-regulatory activities.

It is difficult to determine how many companies participated in the BBBOnline privacy program. A 2000 Federal Trade Commission report on online privacy said that "[o]ver 450 sites representing 244 companies have been licensed to post the BBBOnLine Privacy Seal since the program was launched" in March 1999.[102] Whether the numbers increased in subsequent years is unknown, but the number reported in 2000 clearly represent a tiny fraction of websites and companies. It may be that the more rigorous requirements that BBBOnline asked its members to meet was a factor in dissuading many companies from participating.

BBBOnline stopped accepting applications for its privacy program sometime in 2007.[103] The specific reasons the program terminated are not clear, but it seems likely that it was the result of lack of support, participation, and interest. Self-regulation for the purpose of avoiding real regulation is one thing, but the active and substantial self-regulation offered by BBBOnline may have been too much for many potential participants. BBBOnline continues to operate other programs, including an EU Safe Harbor dispute resolution service,[104] but there is no evidence on its website of the original BBBOnline privacy program. Interestingly, some companies continue to cite the now-defunct BBBOnline privacy program in their privacy policies.[105]

---

[101] See, e.g., http://web.archive.org/web/20070124235138/www.bbbonline.org/privacy/dr/2005q3.asp (last visited 9/20/11). While the BBBOnline privacy program dispute procedures were better and more transparent than other comparable procedures, the BBBOnline dispute resolution service was controversial in various ways. In 2000, for example, questions were raised when the BBBOnline Privacy Program, under pressure from the subject of a complaint, vacated an earlier decision and substituted a decision more favorable to the complaint subject.

[102] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report To Congress* 6 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited 9/20/11).

[103] http://web.archive.org/web/20070830164536rn_1/www.bbbonline.org/privacy (last visited 2/10/11).

[104] http://www.bbb.org/us/european-union-dispute-resolution (last visited 9/20/11). It is not clear if BBBOnline has actually handled any US-EU Safe Harbor complaints.

[105] See, e.g., the Equifax Online Privacy Policy & Fair Information Principles, http://www.worldprivacyforum.org/pdf/equifaxprivacypolicydec5.pdf (last visited 9/20/11); Good Feet, http://goodfeet.com/about-us/privacy-policy (last visited 9/20/11).

III. Discussion: Government Privacy Self-Regulatory Activities

This section reviews several other privacy self-regulatory activities that share some characteristics with the industry self-regulatory programs discussed above, but these activities differ in various ways. The most noticeable differences are the role of the government in the programs. The Department of Commerce is involved in the Safe Harbor Framework, and the Federal Trade Commission is involved in the Children's Online Privacy Protection Act.

Department of Commerce Safe Harbor Framework[106]

The Safe Harbor Framework operated by the Department of Commerce started in 2000 with an agreement between the Department and the European Commission.[107] The Safe Harbor Framework differs somewhat from the other self-regulatory activities discussed in this report because of the role played by the Department. However, the Department's role in the Safe Harbor Framework did not prevent the deterioration of the Safe Harbor over time or stop the lack of compliance by companies that participated in the Safe Harbor.

With the adoption of the European Union's Data Protection Directive[108] in 1995 and its implementation in 1998, much of the concern about transborder data flows of personal information centered on the export restriction policies of the Directive. Article 25 of the Directive generally provides that exports of personal data from EU Member States to third countries are allowed if the third country *ensures an adequate level of protection*.[109]

---

[106] This summary is adapted from an analysis of the Department of Commerce's international privacy activities published by the World Privacy Forum in 2010. The WPF report is The US Department of Commerce and International Privacy Activities: Indifference and Neglect. The WPF report contains additional citations and support for the conclusions presented here. See: http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (last visited 9/20/11).

[107] All Safe Harbor documents can be found at http://www.export.gov/safeharbor/eg_main_018237.asp (last visited 9/20/11).

[108] Council Directive 95/46, art. 28, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281/47), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited 9/20/11).

[109] Other grounds for data exports are not relevant here.

While the EU determined that some countries (e.g., Argentina, Canada, and Switzerland) provide an adequate level of privacy protection according to EU standards, the United States has never been evaluated for adequacy or determined to be adequate.

Restrictions on exports of personal data from Europe created some significant problems and uncertainties for both US and EU businesses, including online businesses. Pressured by the American business community, the Commerce Department intervened to resolve the threats to US business presented by the Data Protection Directive.

The Safe Harbor framework[110] was the result. It allows US organizations to publicly declare that they will comply with the requirements. An organization must self-certify annually to the Department of Commerce in writing that it agrees to adhere to the Safe Harbor's requirements. There are seven areas of privacy standards covering notice, choice, onward transfer (transfers to third parties), access, security, data integrity, and enforcement. Safe Harbor documentation describes the requirements and provides an interpretation of the obligations.[111] To qualify for the Safe Harbor, an organization can (1) join a self-regulatory privacy program that adheres to the Safe Harbor's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the Safe Harbor. The Safe Harbor Framework has its own standards, voluntary certification, and some external method of enforcement so that it is similar to the self-regulatory activities considered earlier this report.

The International Trade Administration of the Department of Commerce now operates the Safe Harbor framework. The Commerce Department website maintains a list of organizations that filed self-certification letters. Only organizations that are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation are eligible to participate. This limitation means that many companies and organizations that transfer personal information internationally cannot qualify for participation either in whole or in part.

Three studies of the Safe Harbor Framework were conducted since the start of Safe Harbor. The first study was conducted in 2001 at the request of the European Commission Internal Market DG.[112] The second study, completed in 2004, was also conducted at the request the European Commission Internal Market DG. An international

---

[110] http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last visited 9/20/11).

[111] http://www.export.gov/safeharbor/eu/eg_main_018493.asp (last visited 9/20/11).

[112] *The Functioning of the US-EU Safe Harbor Privacy Principles*, (September 21, 2001). This study was reportedly published by the European Commission, but a copy has not been located on the EU's data protection webpage or elsewhere on the Internet. The study author is not identified in the document, but a Commission official publicly identified Professor Joel R. Reidenberg, Fordham University Law School, as the author, and the 2004 Study also identified Professor Reidenberg as the author. See 2004 Study at note 2.

group of academics conducted the study.[113] The third study was prepared by Chris Connolly, director of an Australian management consulting company with expertise consultants in privacy, authentication, electronic commerce, and new technology.[114]

Overall, the three studies found the same problems with Safe Harbor. Companies that claim to meet the Safe Harbor requirements are not actually in compliance with those requirements. Evidence from the three reports suggests that the number of companies not in compliance has increased over time.

There is no evidence of improvement in the administration of the Department's Safe Harbor activities. Perhaps the most prominent response to the reports of noncompliance was the addition of a disclaimer on the Department's Safe Harbor website indicating that Department cannot guarantee the accuracy of the information it maintains.[115] It appears that the Department has made some changes to its website over the years, but there remains a lack of evidence of any substantive efforts by the Department to monitor or enforce compliance.

While the Safe Harbor Framework is not a pure industry-run self-regulatory activity because of the role of the Department of Commerce, it shares characteristics of industry self-regulatory activities, namely interest in the Safe Harbor Framework diminished over time, and business support and participation deteriorated. Enforcement has been rare, and the Department never conducted or required audits of participants.

The shortcomings of the Safe Harbor Framework have come to the attention of some data protection authorities in Europe. In April 2010, the Düsseldorfer Kreis, a working group comprised of the 16 German federal state data protection authorities with authority over the private sector, adopted a resolution applicable to those who export data from

---

[113] Safe Harbour Decision Implementation Study (2004), http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf (last visited 9/20/11). As identified in the paper, the authors are Jan Dhont, María Verónica Pérez Asinari, and Prof. Dr. Yves Poullet (Centre de Recherche Informatique et Droit, University of Namur, Belgium) with the assistance of Prof. Dr. Joel R. Reidenberg (Fordham University School of Law, New York, USA) and Dr. Lee A. Bygrave (Norwegian Research Centre for Computers and Law, University of Oslo, Norway).

[114] *The US Safe Harbor - Fact or Fiction?* (2008), http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (last visited 9/20/11).

[115] See https://www.export.gov/safehrbr/list.aspx (last visited 9/20/11) ("In maintaining the list, the Department of Commerce does not assess and makes no representations to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.").

Germany to US organizations that self-certified compliance with the Safe Harbor Framework. The resolution tells German data exporters that they must verify whether a self-certified data importer in the US actually complies with the Safe Harbor requirements.[116]

Essentially, the action by the German state data protection authorities rejects in significant part the Safe Harbor Framework, particularly the self-certification as it appears on the Department of Commerce website. The Düsseldorfer Kreis makes this clear when it states that the reason for its action is that "comprehensive control of US-American companies' self-certifications by supervisory authorities in Europe and in the US is not guaranteed…"[117]

The Department has ignored repeated evidence that many or most Safe Harbor participants are not in compliance with the requirements. Instead, in a recent green paper, the Department claimed that the Safe Harbor Framework was "successful."[118] It is not clear what standard the Department used to measure the success of the Safe Harbor Framework. All available evidence strongly suggests a substantial lack of compliance with the Safe Harbor Framework.

Children's Online Privacy Protection Act (COPPA)

The safe harbor provision in the Children's Online Privacy Protection Act (COPPA)[119] is sometimes cited as a self-regulatory program. For that reason, COPPA is discussed here. However, it is crucial to note that COPPA self-regulation is significantly different from the others discussed in this report. The companies in a COPPA safe harbor must follow all the substantive standards established in the COPPA statute and FTC regulations, meaning that a participant in a safe harbor program must do everything that a non-participant must do *plus* bear the cost of the safe harbor. The standards cannot be changed by the participants in the self-regulatory program. The FTC formally oversees and approves COPPA safe harbor

---

[116] Supreme Supervisory Authorities for Data Protection in the Nonpublic Sector (Germany), E*xamination of the Data Importer's Self-Certification According to the Safe-Harbor-Agreement by the Company Exporting Data* (revised version of Aug. 23, 2010), http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf?1285316129 (last visited 9/20/11).
[117] Id.
[118] Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* at 44 (undated; released in December 2010), http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf (last visited 9/20/11).
[119] 15 U.S.C. §§ 6501-6506.

programs, a characteristic that other self-regulatory programs reviewed here lacked.[120]

In effect, the COPPA safe harbor programs mostly engage in limited enforcement of the statute and relieve the Commission of some of the burden. This may have some benefits overall. It should not be surprising that industry participation in the safe harbor aspect of COPPA is limited. Whether COPPA self-regulation is a success or failure is a subject for reasonable debate, but COPPA has fewer characteristics of failure than the industry self-regulation discussed earlier. For example, there is a formal input procedure for consumers, the safe harbor program has not disappeared, and there has been COPPA enforcement by the FTC. The COPPA model does not appear to be a model in current use outside of this instance. The reason may be that self-regulatory activities under a legislative scheme have little attraction when the principal purpose of industry self-regulation for privacy has been avoidance of regulation in the first place.

IV. Discussion: Combination Self-Regulatory Efforts

The self-regulatory efforts in this category include projects that have many components, including input from government, industry, academia, and civil society.

Platform for Privacy Preferences Project (P3P)

The Platform for Privacy Preferences Project (P3P) is a technical standard for communicating the privacy policies of a website to those who use the website. A user can retrieve a standardized machine-readable privacy policy from a website and use the information to make a decision about how to interact with the website. Each user can match the privacy policy against the user's individual privacy preferences.

P3P allows a browser to understand a website privacy policy in a simplified and organized manner, without the need for a user to find and read a lengthy privacy policy. With the proper browser settings, P3P will automatically block any cookies from a website with a privacy policy that the user determined to be objectionable.

The Center for Democracy and Technology (CDT) supported the early work that eventually resulted in P3P.[121] CDT convened an Internet Privacy Working Group that drafted a mission statement, with companies, trade associations, and consumer

---

[120] 15 U.S.C. § 6503.

[121] For a fuller history of P3P and details on the actual technical standard, see Lorrie Faith Cranor, Web Privacy with P3P (2002).

groups participating. A presentation of a prototype was presented at an FTC Workshop in 1997.[122]

Later in the same year, P3P became a project of the World Wide Web Consortium (W3C), the main international standards organization for the World Wide Web. The working group included representatives of companies, academia, and government.[123] The work of drafting the formal specification took some time, and version 1.0 was finally published at the end of 2000.[124] A later specification was published in 2006.[125]

Microsoft included some support for P3P in its browser, Internet Explorer.[126] The Firefox browser from Mozilla also provides some support.[127] The E-Government Act of 2002[128] included a requirement that federal agency websites translate privacy policies into a standardized machine-readable format,[129] and P3P is the only specification that meets the requirements.[130] It was a promising start.

However, the extent to which commercial websites and even government websites attempted to implement P3P or succeeded in doing so in the long term is highly uncertain. A 2008 published review of P3P by Professor Lorrie Faith Cranor found P3P adoption increasing overall but that P3P adoption rates greatly vary across industries. Other findings are that P3P had been deployed on 10% of the sites returned in the top-20 results of typical searches, and on 21% of the sites in the top-20 results of e-commerce searches. Review of over 5,000 web sites in both 2003 and 2006 found that P3P deployment increased over that period, although there were decreases in some sectors. The review also found high rates of syntax errors among P3P policies, but much lower rates of critical errors that prevent a P3P user agent from interpreting them. Privacy policies of P3P-enabled popular websites were

---

[122] Id. at 45.
[123] Id. at 46.
[124] Id. at 53.
[125] http://www.w3.org/TR/P3P11 (last visited 9/20/11).
[126] See http://msdn.microsoft.com/en-us/library/ms537343%28VS.85%29.aspx (last visited 9/20/11).
[127] See http://www-archive.mozilla.org/projects/p3p (last visited 9/20/11).
[128] Public Law 107-347.
[129] See Office of Management and Budget, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (2003) (M-03-22), http://www.whitehouse.gov/omb/memoranda_m03-22 (last visited 9/20/11).
[130] See, e.g., Department of Health and Human Services, *HHS-OCIO Policy for Machine-Readable Privacy Policies* at 4.2 (Policy 2010-0001, 2010), http://www.hhs.gov/ocio/policy/hhs-ocio-2010_0001_policy_for_machine-readable_privacy_policies.html (last visited 9/20/11).

found to be similar to the privacy policies of popular websites that do not use P3P.[131]

An analysis published two years later by the CyLab at Carnegie Mellon University looked at over 33,000 websites using P3P compact policies and "detected errors on 11,176 of them, including 134 TRUSTe-certified websites and 21 of the top 100 most-visited sites."[132] The study also found thousands of sites using identical invalid compact policies (CP) that had been recommended as workarounds for Internet Explorer cookie blocking. Other sites had CPs with typos in their tokens, or other errors. Fully 98% of invalid CPs resulted in cookies remaining unblocked by Internet Explorer under its default cookie settings. The analysis concluded that it "appears that large numbers of websites that use [compact policies] are misrepresenting their privacy practices, thus misleading users and rendering privacy protection tools ineffective."[133] The study concluded that companies do not have sufficient incentives to provide accurate machine-readable privacy policies.[134]

In other words, the self-regulatory aspects of P3P do not appear to be working, with the CyLab study suggesting that lack of enforcement by regulators is a problem.[135] Neither P3P nor any industry trade association offers a P3P enforcement method.

P3P has some of the indicia of industry self-regulation in that it was inspired in part by FTC interest and motivated in part by an industry interest in avoiding legislation or regulation.[136] The involvement in P3P's development and promotion by consumer groups and the White House together with industry representatives differentiates P3P from the other industry efforts discussed earlier in this report. Another differentiator is the legislative requirement that federal agencies use P3P or similar technology. P3P shares sufficient characteristics with the self-regulatory programs discussed in this report to warrant its inclusion here.

---

[131] Lorrie Faith Cranor et al., *P3P Deployment on Websites*, 7 Electronic Commerce Research and Applications 274-293 (2008).
[132] Pedro Giovanni Leon et al, *Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens* (CMU-CyLab-10-014 2010), http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab10014.pdf (last visited 9/20/11).
[133] Id.
[134] Id. at 9.
[135] Id.
[136] See, e.g., Simson Garfinkel, *Can a labeling system protect your privacy?*, Salon (July 11, 2000), http://www.salon.com/technology/col/garf/2000/07/11/p3p (last visited 9/20/11) ("But P3P isn't technology, it's politics. The Clinton administration and companies such as Microsoft are all set to use P3P as the latest excuse to promote their campaign of "industry self-regulation" and delay meaningful legislation on Internet privacy.").

Some privacy groups opposed P3P from the beginning, largely because of concerns that it would prevent privacy legislation from passing. Company views of the project also varied.[137] It is not clear how much attention P3P has received in recent years from companies or privacy groups.

Unlike some of the self-regulatory activities discussed in Part II of this analysis, P3P remains in use. However, given the findings of the 2010 study of widespread misrepresentation of privacy policies by those using P3P, it is hard to call P3P any kind of success. Further, the study provides strong evidence of deliberate deception in implementation of P3P at some websites. Internet users appear to have little knowledge of P3P, although public awareness may not be essential since the controls are built into browsers and users appear to be concerned about the privacy policies that P3P is designed to convey.[138] Like the Commerce Department's Safe Harbor Framework, P3P continues to exist, but both programs are so lacking in rigor and compliance that neither is fulfilling its original purpose.

V. Conclusion

Is there any reason to think that privacy self-regulation will work today when it did not work in the past? Privacy self-regulation done in the same way that it has been done in the past, without sufficient consumer participation, and with the same goals of simply evading real regulation and effective privacy controls will continue to fail.

What should be done if privacy self-regulation cannot succeed is beyond the scope of this report. This report does not advocate for regulation or against improved self-regulation. The point is that there is no reason to believe that *this time will be different* when it comes to privacy self-regulation done in ways that have been proved to lead to failure. New approaches are needed if the goal is to offer consumer valuable, effective, and balanced privacy protections that last.

What is at stake: Implications for current privacy self-regulatory efforts

If privacy self-regulation today is constructed in the same way as in the past, will it fail in the same way as before? Questions abound. Should self-regulation cover website advertisers? Internet service providers? Data brokers? Social networking sites? Companies using location information? Apps providers? All websites? Defining the Internet universe is daunting, and even within slices of that universe, definitions and boundaries will be difficult to establish. The past history of even the

---

[137] Lorrie Faith Cranor, Web Privacy with P3P 56 (2002).
[138] See Serge Egelman et al., *Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators* (2009), http://www.guanotronic.com/~serge/papers/chi09a.pdf (last visited 9/20/11).

best-intentioned of self-regulatory efforts shows how quickly policy can be outdated by industry and Internet developments.

The web is changing too rapidly to expect that any given form of traditional industry-supported privacy self-regulation will make sense in a year or two. Companies track the activities of individuals today in ways that were not contemplated even a year or two ago. Companies often have no reason to expose to public view their data processing functions for definition or measurement lest they reveal a marketplace advantage.

In most areas of online activity that involve personal information, the number of companies is unknown and highly variable. To determine the penetration of self-regulation coverage, there has to be both a known, demonstrable denominator of companies that fall within the self-regulatory scheme and a numerator of those companies that are participating in the scheme. Without this basic information, there is no real way to measure the penetration of privacy self-regulation. For example, if a list of Internet advertising companies exists at all, that list will go out of date almost immediately. Thus, it is difficult to determine what percentage of the defined universe has agreed to any specific self-regulatory scheme. Even if it were possible to calculate these numbers for *past* privacy self-regulatory activities, the penetration would likely be low and highly variable over time.

Measuring activity though another measure (rather than the number of companies) would probably require access to information that industry would argue to be proprietary. Thus, it is harder than ever to even make basic judgments about the scope and effect of any industry-supported privacy self-regulation.

There is more at stake financially today. Revenues from personal data activities are huge. If a self-regulatory scheme had any real effect on revenues or profits, those who stayed out of the scheme could profit at the expense of those who participated. It is hard to see how a *race to the bottom* effect would be avoided. Still, because there are so many companies and so much money involved in the Internet space, only a small percentage of companies need to participate in a privacy self-regulatory scheme to provide an impressive amount of resources that will make the self-regulation look better than it is. Millions for show, but pennies for substance.

A poorly designed privacy self-regulation scheme that has limited market penetration and insufficient enforcement may be good enough to fool potential regulators once again. Industry is well aware that a little will go a long way for public relations purposes. Industry knows that it only needs to keep a self-regulatory program alive for a limited period. Current debates about privacy self-regulation do not place the burden on industry to prove how proposed self-regulatory privacy programs are going to be substantively different than past efforts, at least in public view.

The Federal Trade Commission has no effective means of issuing privacy regulations because of current limits on its statutory authority. This is a structural problem that essentially compels the agency to look favorably at self-regulation because it has no alternative to offer. The FTC can always recommend legislation, but it is not clear that an FTC recommendation will be influential, that privacy legislation can pass the Congress, or that the FTC can manage to support any legislative recommendation.

Privacy self-regulation as supported by industry today suffers from the same lack of tension as in the past. Without meaningful, independent participation (e.g., by privacy and consumer advocates) in the development and oversight of privacy self-regulation, the self-regulatory standards and enforcement will be just as insufficient as they were in the past. Industry-financed oversight will not succeed because industry does not want it to be effective. For-profit privacy standards will not succeed because the pressure for profits overwhelms the efforts of would-be enforcers.

Privacy self-regulation cannot be meaningful if companies are free to drop out of any self-regulatory scheme at will or to join a different self-regulatory scheme that has weaker standards.
Would-be self-regulators are not likely to sue former members. Privacy commitments typically come with a caveat that they can be changed at will at any time without notice. For-profit companies overseeing privacy standards will not be likely to discipline paying members effectively lest they lose revenues or deter participation from new players.

The threat of Federal Trade Commission action is loudly touted by self-regulators as an effective enforcement method. Reliance on Commission enforcement of self-regulation is a challenge, as industry knows that the Commission does not have the resources to enforce a self-regulation scheme covering hundreds or thousands of companies.

This is the case notwithstanding the absence of meaningful Commission activity against those who ignored or discontinued privacy self-regulation. How can the Commission take action against an industry-supported self-regulatory program that has lost all industry support?

The history lesson here poses challenges to the present efforts for codes of conduct or self-regulation. Self-regulation, done in the same ways as it has been done in the past, is not a hopeful way forward. However, the history lesson is not without hope. This report notes key factors that have been salient in the self-regulatory failures. These factors need to be studied *and* avoided. This report also notes factors that might lay groundwork for success, gleaned from observation of what has not worked. No matter what, one thing is quite certain: there is no need to repeat the past again.

What Could Improve the Process?

It is not the primary purpose of this report to put forward a set of criteria for a meaningful and effective privacy self-regulatory regime. However, it is clear from past experience that some approaches are more likely to produce more positive results and some are not likely to result in a change from the past. In looking at past challenges to success (lack of membership, short duration, no consumer representation, etc.) we are able to set out some basic qualities needed for improvement.

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.

*****

A Note on Methods

This historical review of privacy self-regulation is based on an extensive literature review, both online and offline, and includes information that was publicly available. This report covers the leading self-regulatory efforts. Some self-regulatory efforts may have disappeared without leaving a public record. Also, privacy seal programs arose during the period of this review, but some disappeared entirely and none developed sufficient credibility or public recognition to warrant investigation in this report beyond those noted in the report. Some activities within existing trade associations are difficult or impossible to assess from evidence available to those outside the associations.

Publication Information

This report was published October 14, 2011. The full report is available at www.worldprivacyforum.org/pdf/WPFselfregulationhistory.pdf. Any updates to the report will be posted to this URL.