U.S. Senate Committee on Commerce, Science & Transportation

Hearing: "The Need for Privacy Protections: Is Industry Self-Regulation Adequate?"

Peter Swire
C. William O'Neill Professor of Law
Moritz College of Law
The Ohio State University

June 28, 2012

Chairman Rockefeller, Ranking Member Hutchison, and distinguished Committee Members, thank you for inviting me to testify on "The Need for Privacy Protections: Is Industry Self-Regulation Adequate?"

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. I began working on privacy and self-regulation in the mid-1990's. In 1999 I was named Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that role, I was the first (and thus far the only) person to have government-wide responsibility for privacy policy. As Chief Counselor for Privacy, I worked on both government regulation and self-regulation initiatives to protect privacy while meeting other societal goals. Since then, I have continued to write and speak extensively on privacy and security issues.

For this testimony, Committee Staff requested that I provide historical context about self-regulation and privacy. I was also asked to discuss the Digital Advertising Alliance's recent announcements with respect to Do Not Track, including the exceptions included in the DAA approach. In preparing this testimony, I have spoken at length with industry leaders, privacy advocates, and technologists. This testimony reflects my personal views as a law professor, a former government official, and a person who tries to help develop effective privacy practices in the U.S. and globally.

This testimony has four sections, with the key points set forth in the introduction:

1) **The threat of government regulation spurs the adoption of self-regulation.** In 1997 I presented a paper on privacy and self-regulation at a conference hosted by the U.S. Department of Commerce in which I explained that self-regulation works best when there is a credible threat that government will step in if industry does not do a good job. Simply put, the

industry dynamic around self-regulation is entirely transformed when there is a credible threat of government intervention.

2) **The history of self-regulation after the 1990's shows that self-regulation declined when the credible threat of government action eroded.** When public policy attention shifted away from privacy after the first wave of effort in the 1990's, there was little new progress in self-regulation to match technological change. Indeed, critics who have examined the history have found greatly reduced effort in self-regulation. Some self-regulatory efforts continued, and initiatives that were linked with ongoing government involvement seem to have endured more than others.
3) **The current wave of attention to online privacy has produced progress on Do Not Track, but with broad exceptions to the announced collection limits.** The Digital Advertising Alliance's recent announcement that members would honor a Do Not Track header is potentially important to providing users with choice about their privacy online. However, the current exceptions for market research and product development swallow the Do Not Track rule. In addition, counsel for the DAA has informed me that they are open to concrete discussion about how to further improve these definitions in practice.
4) **We should focus more attention on technical and administrative measures for de-identification in online privacy.** The testimony concludes with a brief discussion of an area for possible win/win scenarios when it comes to privacy and beneficial uses of data online. The idea is simple – technical and administrative safeguards can help ensure data is collected and used in ways that are not linked to the individual.

In summary, there is currently strong attention on the part of Congress, the White House, and the Federal Trade Commission to Do Not Track and privacy issues for online advertising. With this public attention, now is the best opportunity to craft a good regime. When Do Not Track and related efforts are completed, there will be a temptation for policy makers to move onto other issues. That is why it is so important for the current Do Not Track standards and other current initiatives to be as well thought out as possible.

The Threat of Government Regulation Spurs the Adoption of Self-Regulation.

In 1997 Secretary of Commerce William Daley and the National Telecommunications and Information Administration hosted a conference on "Privacy and Self Regulation in the Information Age." My paper for that conference, entitled "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information,"[1] emphasized that self-regulation works best when there is a credible threat that government will step in if industry does not do a good job. Simply put, the threat of government regulation is what spurs the adoption of self-regulation. As discussed in the next section, this conclusion matches the historical experience in privacy self-regulation.

Self-regulation in privacy is a potentially useful approach where there are significant market failures as well as governmental failures. The 1997 paper highlighted a market failure that still applies to today's online advertising market: "A chief failure of the market approach is that customers find it costly or impossible to monitor how companies use personal information. When consumers cannot monitor effectively, companies have an incentive to over-use personal information: the companies get the full benefit of the use (in terms of their own marketing or the fee they receive from third parties), but do not suffer for the costs of disclosure (the privacy loss to consumers)."

The challenge for consumers to monitor online collection of data today in many ways is greater than it was for consumers in 1997. During that period, the Internet was dominated by first-party sites, where the user decided to surf at a particular website that might collect data. Today, collection by third parties is famously complex.[2] News stories in the Wall Street Journal "What They Know" series and elsewhere have shown that even the savviest users find it difficult to opt out of online tracking in a world where cookies respawn and a typical web page can send data to literally dozens of different companies.

Along with these market imperfections, we know that government solutions are imperfect as well. Statutes and regulations are often slow to update to changed circumstances. Needed statutes sometimes face gridlock. Rules can be over-broad (prohibiting net beneficial uses) and under-broad (permitting uses that consumers would object to in the market if they knew about them).

These imperfections in market and regulatory approaches have repeatedly led those in the privacy debate to search for a third way, often called "self-regulation." There are circumstances where self-regulation may be better than the alternative approaches. For instance, self-regulation is more tempting the greater the market and government regulatory failures. Some other factors that tend to favor self-regulation include:

- Industry expertise that leads to better-informed rules;
- Use for technical standards where many participants benefit from cooperation (i.e., network effects from adoption of standards for inter-connection or other purposes);
- Protections against using self-regulation for cartel or other anticompetitive purposes;
- Incentives for the industry to enhance its reputation by adopting and complying with a self-regulatory regime; and
- Effective mechanisms for enforcement through legal, reputational, or other means.

We must also be realistic about the limits of self-regulation. Sometimes self-regulation has been chosen where those involved believed a statute or regulation

would do a better job – even much-needed bills are often difficult to get through the legislative process, and the Federal Trade Commission lacks Administrative Procedure Act rulemaking authority for most privacy issues. Where obstacles to a law are serious enough, self-regulation may be the second best option.

A credible threat of government action is often the single greatest impetus to self-regulatory codes. Government action shapes the agenda, as we see today with this Senate hearing, and as the White House and FTC have shown on Do Not Track and other recent privacy issues. The threat of government action also transforms the dialogue inside industry meetings. When government is not interested, the person proposing the self-regulatory effort says: "Nothing is forcing us to do this, but the right thing would be to adopt a binding code of conduct." When legislation and regulation are looming, the industry discussion is entirely different: "If we don't do this ourselves, they will do it for us. We'll be stuck with compliance for years to come, so we better have something good to say on this issue."

When the Credible Threat of Government Action Erodes so Do Self-Regulatory Programs

The United States had a "first wave" of privacy policy activity related to the Internet from roughly 1996 to 2000.[3] Internet privacy then became a less prominent issue, especially after the attacks of September 11, 2001 focused national attention on uses of data to fight terrorism. We are now in a "second wave" of major attention to Internet privacy. This section of the testimony discusses lessons learned from what happened after the first wave subsided. *When the credible threat of government action eroded, new self-regulatory activity essentially ceased and many self-regulatory programs eroded as well.*

This pattern matches the classic analysis of the "issue-attention cycle" by political scientist Anthony Downs, who wrote: "American public attention rarely remains sharply focused upon any one domestic issue for very long – even if it involves a continuing problem of crucial importance to society."[4] Downs emphasized that we should expect interest in an issue to wax and wane. Downs' discussion is consistent with the thrust of my 1997 paper: "Over time, however, the legislative threat might ease. Agency attention may be directed elsewhere. As the threat of government action subsides, we might expect that self-regulatory efforts would also become more lax."

Examining the history of self-regulation after 2000, even defenders of self-regulation would agree that there was little new progress to match technological change, while critics are far harsher. Some self-regulatory efforts continued, and initiatives that were linked with ongoing government involvement seem to have lasted longer than others.

The World Privacy Forum has written detailed reports about the failings of self-regulation after 2000.[5] Here are some key conclusions:

- "We now have repetitive, specific, tangible examples of failed self regulation in the area of privacy. These examples are not mere anecdotes – these were significant national efforts that regulators took seriously."
- "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."

Similar conclusions come from Chris Hoofnagle, a law professor at the University of California, Berkeley and co-chair of the annual Privacy Law Scholars Conference. Based on his extensive experience with self-regulation, Hoofnagle wrote the following in 2011: "Self-regulatory groups in the privacy field often form in reaction to the threat of regulation. They create protections that largely affirm their current and prospective business practices. The consumer rights created are narrow. They do not update their standards in response to changes, until the regulatory spotlight returns. Nor do they address new actors that raise similar concerns but fall outside of the self-regulatory regime."[6] Just this week, Professor Hoofnagle released a study of the 100 most popular websites, finding that 21 of them placed 100 or more cookies onto users' computers, with 84% of the cookies placed by third parties.[7]

The World Privacy Forum highlights five prominent examples of self-regulation from the first wave.[8] I quote these important examples verbatim, and then offer observations:

1. **"The Individual Reference Services Group** (IRSG) was announced in 1997 as a self-regulatory organization for companies that provide information that identifies or locates individuals. The group terminated in 2001, deceptively citing a newly passed regulatory law that made self-regulation unnecessary. However, that law did not cover IRSG companies."
2. **"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."
3. **"The Online Privacy Alliance** began in 1998 with an interest in promoting industry self regulation for privacy. OPA's last reported activity appears to have taken place in 2001, although its website continues to exist and shows signs of an update in 2011."
4. **"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 evaporated, the NAI had only two members. Enforcement and audit activity lapsed as well. NAI did nothing to fulfill its promises or keep its standards up

to date with current technology until 2008, when FTC interest increased."

5. **"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."

Based on my own experience and some interviews conducted in the days leading up to this hearing, I offer the following observations on these five prominent examples. These observations are subject to the disclaimer about the limited time I have had to double-check each factual situation:

1. **Individual References Services Group:** A lawyer who worked with the IRSG said that passage of Gramm-Leach-Bliley was indeed the key reason for the group's demise. That law did set new limits on sales by financial institutions to data brokers. It did not, however, directly cover most activities of the data brokers who were members of IRSG. My impression is that the data broker industry felt the political pressure was off by the time the group terminated. FTC Commissioner Julie Brill has recently emphasized the need for new privacy initiatives concerning data brokers.
2. **Privacy Leadership Initiative:** According to published reports at the time of its creation in 2000, the PLI planned to spend $30 to $40 million to support self-regulation rather than have online privacy legislation. Because political attention to the issue soon faded, the sponsors apparently believed there was little reason to continue that level of effort after 2002.
3. **Online Privacy Alliance:** The OPA was highly visible during the privacy debates in 1998-2000. If the online privacy issue had remained prominent, I think it is likely that the OPA would have remained much more active for considerably longer.
4. **Network Advertising Initiative:** A senior person who worked with the NAI confirmed the low membership number (two) by 2002, after the considerable fanfare accompanying negotiation of the NAI code in 1999 and 2000. This source gave a different reason, however, for this decline: the collapse of the online advertising market when the dot.com bubble burst.
5. **BBBOnline Privacy Program.** One source explained its demise this way: "Its business model didn't work." It is unclear what combination of factors contributed to its demise. However, factors likely included a poor fundraising structure along with decreased demand for privacy services and a lack of political pressure for privacy protection.

As with any description of recent history, different observers are likely to emphasize different aspects of this record. My own view, however, is that the most optimistic reasonable view of privacy self-regulation after 2000 was that there was little progress until privacy began to get "hot" again in the last few years. These five prominent self-regulatory examples are consistent with the view that self-

regulatory effort fades as the credible threat of government intervention fades. All of these programs garnered headlines when there was political focus on protecting privacy. All of these programs also disappeared or shrunk substantially when political attention focused elsewhere.

With that said, it is useful to examine areas of self-regulation that persisted after 2000:

1. **Website privacy policies.** I have previously written about the effectiveness of the government efforts in the late 1990's to encourage commercial websites to post privacy policies.[9] Within three years, the portion of commercial sites with privacy policies rose from only 12% to a resounding 90%, without legislation. Commercial websites overwhelmingly continued to post privacy policies through the 2000's, encouraged in part by a 2003 California statute that requires such polices for companies targeting consumers there. The existence of these policies is central to the FTC's ability to bring enforcement actions for deceptive trade practices. It is true, of course, that the quality of privacy policies is variable and often low. But this "self regulatory" practice of having privacy policies has remained in effect, and is now extending to the mobile application space.
2. **CAN-SPAM.** In the late 1990's and early 2000's, responsible companies sending commercial e-mail developed codes of good practice. A fundamental element of these practices was to permit consumer choice about receiving commercial e-mail from a particular company. Congress passed the CAN-SPAM Act in 2003. The law is subject to many criticisms, notably that (as with any law) it does not create a technological blockade against malicious spammers. With that said, I submit that the law has been very successful in a core aspect of consumer choice – CAN-SPAM requires companies to include an easy unsubscribe feature in each e-mail. I personally use this feature regularly, and legitimate companies stop sending me e-mail when I unsubscribe. In this instance, a self-regulatory effort was essentially incorporated into statute, and the unsubscribe feature continues to work. The Direct Marketing Association has also continued with its E-mail Preference Service, going beyond CAN-SPAM minimum requirements.[10]
3. **Safe Harbor.** The U.S.-E.U. Safe Harbor was negotiated in 2000. Companies become subject to the Safe Harbor if they certify their membership to the Department of Commerce, and participants are considered to have "adequate" privacy protections under the E.U. Data Protection Directive. Self-regulation is a prominent part of the Safe Harbor because participants must establish an independent recourse mechanism -- must select a self-regulatory program -- to investigate unresolved complaints.[11] Views about the effectiveness of the Safe Harbor vary widely. My own view is that there was a slow start initially for adoption of the Safe Harbor, but thousands of companies have entered it over time, and its principles are widely used even by companies that have not formally certified. The Safe Harbor has endured fairly well in contrast to the purely private-sector self-regulatory efforts; its

official nature, furthermore, has created a helpful framework for ongoing discussions and conferences for the relevant U.S. and E.U. officials and other stakeholders.

These three examples all feature a mixed model of self-regulation, where self-regulatory codes are a precursor to or component of government action. This mixed model is sometimes called "co-regulation," to emphasize the explicit role the government plays along with industry and other stakeholders. Historical evidence from the first wave of Internet privacy, however, suggests that co-regulatory efforts survived better through the highs and lows of the issue-attention cycle than did pure self-regulatory approaches.

The current wave of attention to online privacy has produced progress on Do Not Track, but with broad exceptions to the announced collection limits.

In the last few years, online privacy has become a hot issue again. Three major industry trends are driving this process: the rise of Facebook and other social media sites; the rapid growth in mobile devices, with their implications for location privacy; and the online advertising issues that are the subject of this hearing.[12] These industry trends have been extensively covered in the press. These technological and market changes have prompted political leaders to respond. The E.U. has promulgated a directive limiting use of online cookies and now its draft omnibus Data Protection Regulation. The Administration issued its Green Paper and now its Consumer Online Privacy Bill of Rights. The FTC has been very active on privacy, and has focused public attention on Do Not Track. Congress has devoted much more time to privacy, including today's hearing.

The issue-attention cycle has returned to online privacy. Predictably, so has self-regulation. The Network Advertising Initiative has recovered from its slump in the early 2000's to reach a record membership and level of activity. The Digital Advertising Alliance has spent an enormous number of hours bringing to the table a wide range of players who have never before worked in such detail on privacy issues. Later this month, the Commerce Department will convene a multistakeholder process to address mobile application privacy issues.

Committee Staff have specifically asked me to discuss the Digital Advertising Alliance's recent announcements with respect to Do Not Track, including the exceptions included in the DAA approach. *In my view, the DAA's announcement to honor a Do Not Track header is potentially important to providing users with choice about their privacy online. In their current form, however, the exceptions for market research and product development swallow the Do Not Track rule. In addition, counsel for the DAA has informed me that they are open to concrete discussion about how to further improve these definitions in practice.*

The DAA is a coalition of online advertising organizations, including the Association of National Advertisers, whose President, Bob Liodice, is testifying here

today. In 2009, the DAA released "Self-Regulatory Principles for Online Behavioral Advertising," which contained principles on education, transparency, consumer control, data security, material changes, sensitive data, and accountability. [13] In November, 2011, the DAA released "Self-Regulatory Principles for Multi-Site Data," which extended the 2009 principles beyond online behavioral advertising and also defined a number of important exceptions. In connection with the White House privacy event in February, the DAA agreed that its members would comply when consumers selected Do Not Track in their browsers, with enforcement by the FTC.[14]

These actions by the DAA have accompanied lengthy negotiations on a standard for Do Not Track in the World Wide Web Consortium (W3C). The W3C is a respected organization that has been instrumental to promulgation of many of the technical standards at the core of the modern Internet. The W3C process has involved privacy advocates, technologists, and industry leaders, including members of the DAA. I have not personally attended the W3C meetings, but I have stayed in close contact with participants from all the major perspectives. The W3C working group met for three days last week in Seattle. Although there has been important progress toward consensus on some issues, the scope of the exceptions has remained controversial, including but not limited to the exceptions for market research and product placement.

To place these exceptions in context, the consumer control part of the 2009 DAA principles enables "users of Web sites at which data is collected for online behavioral advertising purposes the ability to choose whether data is collected and used or transferred to a non-affiliate for such purposes." The 2011 DAA principles go further by saying that third parties and service providers "should provide consumers with transparency and consumer control" for purposes other than online behavioral advertising. Along with these limits on collection of multi-site data, the 2011 principles restrict the use of multi-site data for eligibility for employment, credit, health care, or insurance.

The 2011 principles contain important exceptions to the general rule of transparency and consumer control. One category of exceptions is for "operations and system management purposes." Those purposes appear quite broad: "intellectual property protection; compliance, public purpose and consumer safety; authentication, verification, fraud prevention and security; billing or product or service fulfillment; or Reporting or Delivery." There is also an exception for data that will go through a de-identification process, as discussed further below.

I will focus my remarks on the remarkably broad exceptions in the 2011 DAA principles, "for market research or product development." These exceptions are so open-ended that I have not been able to discern any limits on collection under them. Market research includes "research about consumers."[15] That would seem to include keeping track of every click made by a consumer. Market research also includes analysis of "consumer preferences and behaviors." Again, if I were an FTC enforcer, I don't know what lies outside the scope of the exception. The definition of

product development is similarly broad. It includes analysis of "the characteristics of a market or group of consumers." To analyze a "group of consumers" would seemingly permit collecting each click made by those consumers. Similarly, product development includes analysis of "the performance of a product, service, or feature."

The 2011 DAA principles place one limit on information collected under the market research and product development exceptions. They state that the terms do not "include sales, promotional, or marketing activities directed at a specific computer or device." Thus, companies should not collect information from Alice or Bob under the exceptions, and then use their specific knowledge about Alice or Bob to target their computers or other devices. The scope of this consumer protection, however, is currently unclear. The principles do permit any contact back to the computer of Alice or Bob "based on an aggregate use of data." The current principles do not offer further guidance on what is permitted based on that aggregate use of data.

After reading the text of these exceptions to prepare this testimony, I then spoke about experts from both industry and the advocacy community to test the accuracy of my reading. My understanding, under the 2011 DAA principles, is that under the market research and product development exceptions:

- Companies have no transparency requirement;
- Companies have no consumer choice requirement;
- Companies can keep the data indefinitely;
- Companies can identify data that is collected without the user's name, and combine it with identified data;
- Companies can combine their data with data from other sources, to build up a more detailed profile; and
- Companies can share data with other third parties so long as it is not used to market back to the specific computer or device.

To summarize, the 2011 DAA principles have a section called "Limitations on the Collection of Multi-Site Data." The market research and product development exceptions are part of that section. As drafted, it is difficult to see what limitations on collection could be enforced given the breadth of the exceptions.

What should be done in light of these findings? The counsel for the DAA, has informed me that they are open to concrete discussions about how to further improve these definitions in practice. Counsel specifically understood that I would state that in this testimony.

My view is that considerably more work needs to be done in defining the market research and product development exceptions. As one person, I don't presume to know the answers to these complex questions. I do believe, however,

that participants can get helpful insights from the way that market research and research generally have been handled in other contexts that implicate privacy. For instance, telephone market research has existed for decades. My understanding is that there are well-developed practices, and perhaps codes of conduct, for protecting confidentiality in telephone market research. To my knowledge, there have not been recent scandals about whether Gallup or some other research firm has re-identified an individual's response to a telephone survey. Based on discussions with participants in the W3C process, these offline market research precedents have not been discussed at the W3C. Perhaps the online community can learn from the historical practice for offline market research.

Similarly, we have extensive experience on how to define and conduct research in other settings. Many federal agencies gather data for statistical research, from the Census to economic statistics and many other purposes. These agencies have years of experience of how to get needed statistical information while preserving confidentiality, and the current online advertising debates should draw on that expertise.[16] Under the HIPAA medical privacy rule, there are at least four methods for conducting research on protected health information: (1) individual consent; (2) de-identification of the data; (3) with authorization from an Institutional Review Board or Privacy Board; or (4) on limited data sets, where the researchers agree to comply with confidentiality conditions in order to get the data.

I am not saying that the rules for medical research should apply online; instead, the point is that *researchers have used data intensively in many settings other than online advertising. The online advertising debates should be better informed by the institutional options that have been developed in areas such as offline market research, government statistics, and medical research*.

Improve & Employ Technical and Administrative Measures for De-Identification in Online Privacy

Before concluding, I will briefly discuss an area where there may be important win/win outcomes both for privacy and beneficial uses of data about online activities. With the Future of Privacy Forum, I am conducting a research project on de-identification in the online advertising space. We have received expressions of interest from industry, privacy advocates, and technologists.

The idea is simple – we should employ technical and administrative safeguards so that data is collected and used in ways that are not linked to the individual. If we can build effective safeguards, then data can be used more intensively while protecting against privacy problems.

Doing de-identification well is a challenging problem, but I believe we are now in a time when more work is needed about how to do it online. In its recent report, the FTC proposed a promising approach to de-identification, which includes technical measures as well as public statements from companies that they will not

re-identify individuals, with those statements being enforceable under the FTC Act.[17] The 2011 DAA principles contemplate greater use of de-identification, where "an entity has taken reasonable steps to ensure that the data cannot reasonably be re-associated or connected to an individual." I have started to write on this topic,[18] and recently submitted comments to the Department of Commerce about how de-identification could be a candidate for a multi-stakeholder process.[19]

Due to its highly technical nature, it is difficult to craft a statute that states specifically how to achieve de-identification. To date, there has not been enough work to understand what mix of technical and administrative safeguards will best protect privacy while also enabling beneficial uses of information. I hope that many parties will focus more attention on how to build de-identification more effectively into our Internet practices.

Conclusion

In conclusion, let me state my optimism about the intelligence, good faith, and willingness to work hard on these issues in industry, the privacy advocacy community, and among technologists. The online advertising eco-system today is much more complex than in the 1990's. There are major institutional challenges in understanding the technology and market forces, and coordinating a response.

In making progress on such issues, we should be informed by the history. When Congress and agencies focus on an issue, the attention often brings out the best in industry. The public attention empowers technologists and other privacy experts within companies and industry groups to convince their colleagues to take effective measures to protect privacy. By contrast, if the pressure is off, the privacy experts within industry find it more difficult to get their colleagues to protect personal information.

Getting online privacy right is important for each of us as Americans. In testimony last fall before the House Energy & Commerce Committee, I explained that a "we don't care about privacy" approach from the United States would create risks for American jobs, exports, and businesses.[20]

More simply, I personally would not like to have an Internet where I believed that each moment of my browsing might easily be breached and shown to the entire world. For you and your families, it would reduce the quality of the Internet if you thought that any page you visited needed to be treated like something that might be released to the public. That is not the experience we have today. However, if we do not foster good practices, then we risk losing confidence in our use of the Internet.

Thank you once again for the invitation to testify today. I am happy to respond to your questions.

Biographical Information

Peter Swire is the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. He began working on privacy and self-regulation in the mid-1990's. In 1998, he was the lead author, with Robert Litan, of "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive," published by the Brookings Institution. In 1999, he was named Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that role, he was the first (and thus far the only) person to have government-wide responsibility for privacy policy.

As Chief Counselor for Privacy, he worked on both government regulation and self-regulation initiatives to protect privacy while meeting other societal goals. On the government regulation side, he was the White House lead on the HIPAA medical privacy rule and on the financial privacy rules implementing the Gramm-Leach-Bliley Act. For self-regulation, he worked extensively in connection with the Network Advertising Initiative code of 2000, and helped negotiate the Safe Harbor agreement for data flows between the E.U. and the U.S., including a major role under the Safe Harbor for self-regulatory associations.

In 2001, Swire returned to law teaching. He has since continued to write and speak extensively on privacy and security issues, with publications and speeches available at www.peterswire.net. In 2009 and 2010 he was Special Assistant to the President for Economic Policy, serving in the National Economic Council under Dr. Lawrence Summers. In 2010, he once again returned to law teaching at The Ohio State University. He lives in the D.C. area.

---

[1] http://ssrn.com/abstract=11472.

[2] A chart of the complex display advertising ecosystem is at page 4 of *Comments of the World Privacy Forum regarding the Federal Trade Commission Preliminary Staff Report "Protecting Consumer Privacy in an Era of Rapid Change,"* (2011), at http://www.ftc.gov/os/comments/privacyreportframework/00376-58005.pdf.

[3] Peter Swire, *Why Privacy Legislation is Hot Now*, Thehill.com, June 23, 2011, at http://thehill.com/component/content/article/72-opinion/168267-why-privacy-legislation-is-hot-now.

[4] Anthony Downs, *Up and Down with Ecology – the "Issue-Attention Cycle,"* 28 Public Interest (Summer 1972), at 38.

[5] Robert Gellman & Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, (2011), at http://www.worldprivacyforum.org/pdf/WPFselfregulationhistory.pdf; World Privacy Forum, *The Network Advertising Initiative: Failing at Consumer Protection and Self Regulation*, (2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

[6] Chris Hoofnagle, *Can Privacy Self-Regulation Work for Consumers?*, Jan. 26, 2011, http://www.techpolicy.com/CanPrivacySelf-RegulationWork-Hoofnagle.aspx.

[7] James Temple, *Web Privacy Census Shows Tracking Pervasive*, SFGate, June 26, 2012, at http://www.sfgate.com/default/article/Web-Privacy-Census-shows-tracking-pervasive-3663642.php.
[8] Gellman & Dixon, supra.
[9] Peter Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 52 Hastings L.J. 847 (2003), at http://ssrn.com/abstract=424167.
[10] http://www.dmaconsumers.org/consumers/optoutform_emps.shtml
[11] See http://export.gov/safeharbor/eu/eg_main_018495.asp.
[12] Peter Swire, *Why Privacy Legislation is Hot Now*, Thehill.com, June 23, 2011, at http://thehill.com/component/content/article/72-opinion/168267-why-privacy-legislation-is-hot-now.
[13] http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf
[14] The White House, *We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online*, Feb. 23, 2012, at http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.
[15] "Market Research means the analysis of: market segmentation or trends; consumer preferences and behaviors; research about consumers, products, or services; or the effectiveness of marketing or advertising. A key characteristic of market research is that the data is not re-identified to market directly back to, or otherwise re-contact a specific computer or device. Thus, the term "market research" does not include sales, promotional, or marketing activities directed at a specific computer or device."
[16] For a history of confidentiality and federal statistics, see Douglas J. Sylvester & Sharon Lohr, *Counting on Confidentiality: Legal and Statistical Approaches to Federal Privacy Law After the USA PATRIOT Act*, 2005 Wisc. L. Rev. 1033.
[17] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012), at http://ftc.gov/os/2012/03/120326privacyreport.pdf.
[18] http://www.peterswire.net/psspeeches2011.htm.
[19] http://www.ntia.doc.gov/federal-register-notice/2012/comments-multistakeholder-process.
[20] Peter Swire, *Internet Privacy: The Impact and Burden of EU Regulation*, Statement before the House Energy & Commerce Committee, Sept. 15, 2011, at http://www.americanprogressaction.org/issues/2011/09/swire_testimony.html.