# Federal Trade Commission

**Privacy Law Scholars Conference**
**Washington, DC**

**Remarks of David C. Vladeck[1]**
**Director, FTC Bureau of Consumer Protection**
**June 3, 2010**

It is an honor for me to be here at this all-star line-up of privacy experts. So many of you in this room have made important contributions to our understanding of how privacy and technology intersect.

As this audience well knows, privacy and technology are inextricably intertwined. When Louis Brandeis and his partner Samuel Warren authored their seminal Harvard law review article on privacy in 1890, they were concerned about the invasive impacts of a new technology – the camera. They wrote that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[2] They were concerned that "unauthorized" photographs of private persons were being

[1]The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner.

[2] Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).

published in irresponsible tabloids. Fortunately, as we all know, irresponsible tabloids are a thing of the past.

Time and again, we've grappled with the fundamental changes wrought by new technologies and the impact those changes have had on personal privacy. In the Fourth Amendment context, new developments in surveillance — such as the wiretap, the pen register, and aerial surveillance and thermal imaging devices — presented thorny issues for courts that were called on to determine whether people had a reasonable expectation of privacy when those expectations were unsettled. The courts often turned to more familiar analogs and extended those concepts to new situations – telegraph wiretaps raised similar issues to phone wiretaps, for example, and something outside that is visible from a low-flying plane might also be visible from a neighboring street.

In the commercial context online, consumers often must come to terms with information practices that are wholly new to them — and often invisible — in part because the pace of innovation in information practices and management in the Internet Age is unprecedented and the light-speed pace of development outstrips the ability of us to keep up.

The Netscape browser first opened the way for commercial use of the Internet just 15 years ago. Since then, geometric increases in computational and data transmission speeds and cheaper and cheaper data storage costs have had huge implications. Thanks in large part to the flow of information that it makes possible, this steady innovation has created stunning benefits to consumers. These advances have also created new risks for consumers, including risks to their privacy.

At the FTC, we are trying to address these risks without stifling the dramatic benefits of technological innovation. We are doing so through policy development and enforcement. I'd like to highlight our activities in each of these areas.

## I. Policy Development

As many of you know, we've been examining the impact of existing and emerging business models on consumer privacy in our series of roundtables. And as I look around the room, I see a good number of people who contributed their time and expertise to this process – we're tremendously grateful for that. Let me highlight some of the key take-aways from the roundtable discussions and the public comments.

First, we heard that, given the sheer volume of information that is now collected and maintained about individuals, it no longer makes sense to talk about "personal information" and "non-personal information." Many of you have conducted ground-breaking studies that drive this point home. So on the Web, and even increasingly offline, it is getting harder for consumers to choose anonymity, if that word still has any meaning.

Second, we talked about the implications of the relatively low cost of maintaining data. We heard from many people that data now is more expensive to destroy than to keep. The implication is that larger and larger databases can be maintained at relatively low cost. And data often outlives the hardware that houses it, increasing the likelihood that the data will hang around long enough that it is re-examined and re-purposed for uses that may not have been contemplated at the point of collection.

Third, because of the fast pace of change, consumers understand very little about how their information is handled and with whom it is shared. New business models arise literally daily, so consumers are often presented with unfamiliar or confusing situations where the trade-

offs in terms of privacy are not clear and are constantly shifting. We are more comfortable with photos appearing in the press today than Warren and Brandeis were in their day, but people haven't had time to come to terms with online information practices.

This confusion by consumers about how their information is handled and shared is prevalent despite the widespread adoption of privacy policies, at least by consumer-facing companies. Again, many of you have demonstrated the limitations of privacy policies in your studies. And of course, consumers know even less about the many other players who have access to their information behind the scenes, including businesses like data brokers, ad networks and application providers.

Finally, we heard loud and clear that people are not satisfied with the policy approaches we've taken to date and with the state of privacy on the Web. Many years ago we encouraged companies to disclose their privacy practices in hopes that informed consumers could make the best choices. Although such disclosures were a useful tool to promote business accountability, we learned that they are not a useful way to communicate with consumers. In practice, privacy policies are not located where consumers need them and they're too complicated, too vague, and too long.

I don't mean to sound gloomy about privacy on the Internet, because I'm not. The technology that drives the Internet is a powerful tool for information dissemination, innovation and collaboration. And with respect to privacy, technology is certainly going to be a big part of any solution. Several companies have already introduced tools that consumers can use to access the interest categories they've been placed in – and to change how they're categorized. A non-profit think tank, the Future of Privacy Forum, together with marketing communications company WPP, has led an effort to develop and test an icon to alert consumers how to get more

information and make choices about how their information is used for behavioral targeting. Many other companies offer privacy-enhancing technologies.

I'm also optimistic because of the dedication and commitment of all the experts here today. The research that you conduct has been enormously valuable in helping us as we evaluate different policy approaches to protect consumer privacy in light of both the risks and benefits of information flows.

* You have made us think about what it means to be anonymous in a world where data from myriad databases can be combined to tease out individuals' identities and preferences.
* You've made us think about how much consumers understand about how their information is shared and how they think about the trade-offs.
* You've made us think about how much people will pay for privacy.
* And you made us think about the growing "commodification" of personal data — that is, that data collected about individuals has a market price, now set by high-tech auctions, and the more "granular" that information, the higher the price. You are making us think about the implications of that marketplace.

You've already helped us so much, but I'd like to ask yet more of you. When we issue our initial report later this year for public comment, we'd really appreciate your input on how to make information practices transparent and understandable, and how to give consumers meaningful choices.

I should note that, not only are we looking at privacy generally, we are also conducting a review of the Children's Online Privacy Protection Rule. In light of rapidly changing technology such as the increased use of smartphones and other devices to access the Internet, we

hosted a public roundtable yesterday to explore whether to update the rule, in light of rapidly changing technology. The COPPA rule was enacted in 2000 and requires Web site operators to obtain parental consent before collecting, using, or disclosing personal information from children under 13. Roundtable topics included:

* whether the rule should be applied to emerging media such as mobile devices, interactive television, and interactive gaming;
* potential expansion of the rule to cover more items of information that might be collected from children; and
* a review of the parental verification methods used by Web site operators.

We are accepting comments as part of our review until June 30. Based on the record, we will determine whether to propose changes to the COPPA rule as well as to the statute itself.

## II. Enforcement

While our policy work on privacy issues is a top priority, I don't want to give the impression that we are doing nothing else. We are still engaging in our core business, so to speak, and that is enforcement. Much of our work is non-public; we have a number of important, open investigations, that I cannot discuss. But we've also resolved a number of important matters recently, and let me mention a few examples.

First, we have engaged in extensive data security enforcement. We have brought 27 cases challenging faulty data security practices by organizations that handle sensitive consumer information. Our most recent data security case was against Dave & Buster's, Inc., an entertainment operation that the FTC charged left consumers' credit and debit card information

vulnerable to hackers, resulting in several hundred thousand dollars in fraudulent charges.[3] The settlement bars deceptive claims and requires Dave & Buster's to establish a comprehensive data security program and obtain biennial independent third-party assessments of that program for twenty years.

Second, we have challenged false claims related to identity theft protection. Earlier this year, we announced a joint FTC-35 state settlement against LifeLock. The FTC's complaint in this case charged that the company used false claims to promote its identity theft protection services, which it widely advertised by displaying the CEO's Social Security number on the side of a truck.[4] But the holes in LifeLock's identity theft protection program were large enough to drive a truck through. This enforcement action is one of the largest FTC-state coordinated settlements on record. The settlements bar deceptive claims and require LifeLock to hand over $12 million dollars. $11 million to the FTC and $1 million to the states. The FTC will use the $11 million it receives from the settlements to provide refunds to consumers.

Third, we have brought actions involving deceptive misrepresentations about self-regulatory programs. We recently settled a case involving a company called ControlScan, which consumers relied on to certify the privacy and security of online retailers and other Web sites. In this case, the FTC alleged that ControlScan misled consumers about how often it monitored the sites and the steps it took to verify their privacy and security practices.[5] ControlScan provided a "seal" to Web sites that they could display, conveying to consumers the pledge that an

---

[3] *FTC v. Dave & Buster's, Inc.* FTC File No. 082-3153 (final order May 28, 2010).

[4] *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz., final order Mar. 15, 2010).

[5] *FTC v. ControlScan, Inc.* (N.D. Ga., final order Feb. 25, 2009).

independent party is auditing their privacy and security practices. We alleged that ControlScan provided the seals to Web sites with little or no verification of their security or privacy protections. The settlement with ControlScan bars future misrepresentations and includes a monetary judgment.

Finally, we continue to investigate companies to determine whether enforcement actions are warranted in new technology areas. For example, we recently announced an initiative in the area of P2P file sharing software. We notified almost 100 organizations that personal information had been shared from the organizations' computer networks through peer-to-peer file-sharing networks. As a result, any users of those P2P networks could access the personal information on them and use it to commit identity theft or fraud. We sent education materials to these organizations on how to secure P2P file sharing software on their networks. We also opened several non-public investigations of other companies whose customer or employee information has been exposed on P2P networks.

As in our policy work, our enforcement efforts rely heavily on the work of academics. For example, last year, we investigated Netflix for its planned release of "anonymized" individual movie queues to the public, in order to develop a better algorithm for recommending movies. In 2006, Netflix had released similar data, and two researchers from the University of Texas were able to demonstrate that it was possible to re-identify individuals using the purportedly anonymized data set, along with minimal additional public information. In light of this research, Netflix's intention to release a second data set raised a serious risk that Netflix's customers could be re-identified and associated with their potentially sensitive movie viewing histories and preferences.

After discussions with FTC staff, Netflix suspended its public release of movie queue information. The company agreed that if it were to release such a data set in the future, it would not do so publicly; rather, it would release it only to researchers who contractually agree to specific limitations on its use. In addition, Netf1ix stated that it would implement a number of operational safeguards to prevent the data from being used to re-identify consumers. We issued a public closing letter in the matter, in which we encouraged companies to be cautious when releasing data presumed to be "anonymous" or "not personally identifiable," especially when those representations are made to consumers.

## III. Conclusion

By concluding my substantive remarks today with a discussion of Netflix, I end where I began – with the intersection of technology, privacy, and academic research. Some may view the work of academics as an "ivory tower" exercise, but I assure you that your work from the tower provides those of us on the ground with an important lodestar to guide our efforts. Your work has informed both our policymaking, as well as our enforcement efforts. We hope we can continue our valuable partnership to ensure that consumers can reap the benefits of technology and maintain their privacy.