Federal Trade Commission

"Promoting Consumer Privacy: Accountability and Transparency in the Modern World"

Remarks of David C. Vladeck, Director, FTC Bureau of Consumer Protection[1]
New York University
October 2, 2009

I. Introduction

Science-fiction writer David Brin once said, "when it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else." Well, as policymakers, we must demand privacy and accountability from everyone. Certainly, businesses and governments must be held accountable: They must respect consumers' privacy in collecting and using data. But individuals also have to take responsibility for the data they share, including the data they post on the Internet.

However, before we can hold consumers accountable in this way, we also need to promote transparency of privacy practices. Consumers need to understand how the information they share will be used, so that they can make informed decisions about whether to share it in the first place. In short, along with accountability for information practices, we need to promote transparency and ways of enabling consumers to exercise meaningful choice.

---

[1]The views stated here are my own and do not necessarily reflect the views of the Commission or any Commissioners.

The Federal Trade Commission is assessing the best ways to promote transparency and accountability in commercial information-handling practices. To this end, we are launching a project to explore new consumer privacy frameworks. As part of this project, the Commission will host a serious of roundtables to get public input on various models for promoting consumer privacy. The first such roundtable will take place on December 7 at FTC Headquarters in Washington, D.C. I invite all of you to attend.

In my remarks today, I'll take a look at the Commission's past privacy initiatives and discuss how they will inform the future. I'll start by briefly discussing the evolution of the Commission's privacy program over the past decade. I'll then discuss some of the lessons we've learned from our most recent initiatives on privacy and how we will apply those lessons in our effort to explore new consumer privacy models.

II. The Commission's Approach to Privacy

Privacy has been one of the Commission's highest consumer protection priorities for more than a decade. The FTC has worked to address privacy issues through consumer and business education, regulation, law enforcement, and policy initiatives. Recognizing the increasing importance of privacy to consumers and to a healthy marketplace, in 2006 the FTC established the Division of Privacy and Identity Protection, devoted exclusively to privacy-related issues.

Over the years, the Commission's goal in the privacy arena has remained constant: To protect consumers' personal information and to ensure that consumers have confidence to take advantage of the many benefits offered by the ever-changing marketplace. Although the goal has been the same, the strategies have evolved to adapt to changing technologies and business practices.

The privacy concerns also have evolved. Some of you may have read the piece in last Sunday's New York Times magazine about middle-schoolers struggling with their sexual orientation. Take the example of one of the adolescents in the article who didn't want to state publicly that he was gay. Suppose he wanted to find information about others in his situation. Just a generation ago, he may have gone to his local library to find this information in the encyclopedia, and emerged with no record of his search. That effort would be anonymous, and would leave no paper trail. There was no privacy debate to be had.

Today, the individual would probably look for information on the Internet. If he does so on his home computer, he may be surprised — indeed, even mortified — to receive advertising based on his searches and to learn that third parties have access to information about his searches. Even if the individual conducts his search at the local library or on a public computer, there may be a record of that search that may be used in ways he did not and probably could not anticipate – after all, he may have had to enter his library card information or credit card number to access the Internet. As this simple example shows, the privacy implications of new technologies are vast.

This example also shows why our policies need to be adaptable. We may not like the fact that our Internet research can be tracked. But I don't think that even the most privacy-sensitive person among us would advocate for going back to the days of library-based encyclopedia research. Thus, the example is a simple demonstration of our shared challenge: To reap the substantial rewards of a digital world without needlessly sacrificing consumer privacy.

III. Exploring New Privacy Frameworks

As we explore new privacy frameworks, we will attempt to draw upon some of the lessons we have learned from our privacy work generally, and in particular, our recent initiatives

to address behavioral advertising. Behavioral advertising benefits consumers in the form of advertising that is more relevant to their interests. It also helps to subsidize and support a diverse range of free online content and services that otherwise might not be available or that consumers would otherwise have to pay for – content and services such as blogging, social networking, and instant access to newspapers and information from around the world.

At the same time, however, behavioral advertising raises consumer privacy concerns. For one thing, it is far from clear that consumers even know that they are being "tracked" when they visit internet sites. And those consumers who understand tracking, may be uncomfortable with being tracked, but may be unable to engage in self-help. In addition, without adequate safeguards in place, consumer tracking data may fall into the wrong hands or be used for unanticipated purposes. These concerns are exacerbated when the tracking involves sensitive information about, for example, children, health, or a consumer's finances.

In November 2007, the FTC held a "Behavioral Advertising" Town Hall to explore the impact of new developments in this area. Based upon the discussions at the Town Hall, FTC staff issued for public comment a set of high-level proposed principles to encourage and guide industry self-regulation.[2] This February, we issued a report that responded to the comments received and fleshed out the principles further.[3] The Town Hall, principles, and report contain several lessons for our ongoing work to explore new privacy frameworks.

A: Lesson 1: Timing is Everything

---

[2] *See* Federal Trade Commission, "Ehavioral Advertising: Tracking, Targeting, & Technology," *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

[3] *See* Press Release, "FTC Staff Revises Online Behavioral Advertising Principles," Feb. 12, 2009.

The first lesson – mainly for policymakers – is that timing is everything. Although the Commission has been examining behavioral advertising for several years, its latest efforts have been successful largely because they have coincided with the emergence of new business models and increased public awareness of the practice. For example, in November 2007, around the time the FTC held its Town Hall on the subject, Facebook released its Beacon program. This program tracked the activities of Facebook users on third party sites. If a user did not opt out of this tracking, Facebook would send information about the user's purchases at these third-party sites to the user's Facebook friends. The Beacon program generated massive publicity and raised significant concerns among Facebook users. In response to public outcry, Facebook changed its program by adding more user controls over what information is shared and by improving notice to users. Just last week, according to press reports, Facebook announced that it will shut down the Beacon service to settle an ongoing lawsuit.[4]

Just as the timing was right for the Commission's work on behavioral advertising, the time is right for re-examining existing models for consumer privacy. New technologies have raised privacy challenges not easily addressed by the existing privacy frameworks. For example, current approaches to privacy revolve around providing consumers with notice and obtaining informed consent to collect and use their information. Where consumers are unfamiliar with new technology and business models, it may be particularly difficult to achieve informed consent. Consumers appear to be constantly caught off guard by the extent to which their

[4] Vijayan, Jaikumar, "Privacy Advocates Hail Facebook's Plan to Shutter Beacon, Computerworld, Sept. 22, 2009, www.computerworld.com/s/article/9138373/Privacy_advocates_hail_Facebook_s_plan_to_shutter_Beacon.

information is collected and shared with third parties. The Beacon example is one example of this. Another example is the rise of third-party applications – because the use of third-party applications on social networking sites is relatively new, many consumers may not be familiar with how such applications could gain access to their data.

Similar challenges arise in the area of P2P file sharing. Recent news reports have highlighted disturbing instances of sensitive documents being shared via P2P networks. These have included documents disclosing avionics details of the President's helicopter,[5] financial information of a Supreme Court Justice,[6] and many thousands of tax returns and medical records of ordinary citizens.[7] In this context, consumers may download P2P software to share music files, knowing that their music files are accessible to others. The consumers (or perhaps more often, their teenage children) might not know, however, that the software can give people access to *all* of the personal data from their computers.

Just like consumers, businesses need guidance on how to protect consumer privacy in the face of new technological developments. For example, as screens get smaller, how do businesses provide adequate disclosures to consumers about privacy issues? I can barely read messages on my Blackberry or cell-phone. And as responsibility for data protection becomes more diffuse – as in the case of cloud computing, where invisible service providers may remotely process and store data – who is responsible for safeguarding it?

---

[5] Cooper, Charles, "Data About Obama's Helicopter Breached Via P2P?" CNET News, Feb. 28, 2009, http://news.cnet.com/data-about-obamas-helicopter-breached-via-p2p.

[6] Krebs, Brian, "Justice Breyer is Among Victims of Data Breach Caused by File Sharing," Washington Post, A01 (July 9, 2008).

[7] Sandoval, Greg, "Congress to Probe P2P Sites Over 'Inadvertent Sharing'" CNET News, Apr. 21, 2009, http://news.cnet.com/8301-1023_3-10224080-93.html.

Moreover, the timing is right to reexamine privacy issues, not only because of advances in technology, but also because of advances in innovative policymaking. We need to take advantage of the momentum that is building around in the United States and around the globe on privacy issues. The House Energy and Commerce Committee is drafting new omnibus privacy legislation, and the Administration is convening meetings to develop positions on privacy. In addition, the new Business Forum on Consumer Privacy, consisting of business leaders from Microsoft, eBay, Google, and Hewlett Packard, has recently formulated a new approach to protecting privacy in the digital economy. And the Ontario Privacy Commissioner has launched a "Privacy by Design" Challenge, through which it has called on companies to embed privacy-enhancing technologies into the architecture of new systems. There is a lot of creative thinking out there, and part of our effort is aimed at getting the best minds engaged in privacy issues — many of them in this room — to meet and come up with the next great idea.

B. Lesson 2: It's not (or shouldn't be) in the fine print.

As we move forward on our plan to explore new privacy frameworks, lesson 2 is that it's not – or at least it shouldn't be – in the fine print, and the print shouldn't be written by lawyers. It is important for privacy practices to be transparent and understandable. Taking the example of behavioral advertising, surveys show that many consumers still have little understanding about the practice. Although consumers' awareness does seem to be improving, one survey showed that still one-third of consumers – a significant minority – do not understand it.[8] Thus, we know that we need to improve transparency in this area.

---

[8] *See* Press Release, Truste Behavioral Advertising Survey, March 2009, http://truste-test.extractable.net/about_TRUSTe/press-room/news_truste_behavioral_targeting_survey.html.

We also recognize that transparency does not mean sticking a fine-print, legalese notice in an obscure link to a privacy policy. Indeed, many companies have developed long privacy policies, terms of service agreements, or end-user license agreements with buried disclosures that consumers cannot find, read, or comprehend. The result is that consumers may not understand how their information is used. This result undermines, rather than furthers, our stated objective of transparency.

A recent Commission enforcement action demonstrates the problems with lack of transparency in privacy policies. This June, Sears agreed to settle an FTC complaint alleging that Sears failed to disclose adequately the scope of consumers' personal information it collected via a downloadable software application. According to the FTC's complaint, Sears paid $10 to consumers who visited their websites and agreed to download "research" software that Sears said would confidentially track their "online browsing." In fact, the software collected vast amounts of information, such as the contents of consumers' shopping carts, online bank statements, drug prescription records, video rental records, and library borrowing histories. Only in a lengthy user license agreement, available to consumers at the end of a multi-step registration process, did Sears disclose the full extent of the information the software tracked. The settlement calls for Sears to stop collecting data from the consumers who downloaded the software and to destroy all data it had previously collected.[9] As this case demonstrates, without real transparency, consumers cannot make informed decisions about how to share their information.

In the context of behavioral advertising, we have encouraged companies to design

---

[9] *In the Matter of Sears Holding Corp.*, FTC Docket No. C-4264 (September 9, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm.

innovative ways – outside of the privacy policy – to provide disclosures to consumers. For example, let's say a consumer gets a targeted ad based on his or her search history. A company could provide an effective disclosure if it includes a link in close proximity to the ad, with the title "Why did I get this ad?" The text in the link could explain how data is collected for purposes of delivering targeted advertising. Indeed, such a disclosure is likely to be far more effective than a discussion – even a clear one – that is buried within a company's privacy policy.

During our upcoming roundtables on privacy, we hope to hear more about innovative approaches to providing effective notice and choice, both online and offline. We also hope to hear directly from those who have done actual consumer testing. This could help us find out what consumers think are the most effective ways for companies to communicate their privacy policies.

C. Lesson 3: Privacy is an important value.

Lesson 3 is that privacy is an important value in itself. In the early to mid-2000s, the Commission focused its privacy agenda on those egregious practices that caused the most tangible harm to consumers, such as physical or economic harm. As a result, it made significant, concrete strides in combating unfair and deceptive practices in the areas of data security and identity theft, children's privacy, spam, spyware, and telemarketing.

Nonetheless, one of the lessons from our work on behavioral advertising is that a focus only on those privacy practices that cause concrete or tangible harm has its limitations. The range of privacy-related harms is not limited to those that cause physical or economic injury or unwarranted intrusion into one's personal time. The actual range of privacy-related harms is wide, and includes reputational harm, fear of being monitored or having private information "out there," or having one's data used in a manner contrary to his or her expectations. Indeed, many

consumers may believe that they have suffered harm when their personal information – particularly sensitive health or financial information – is collected, used, or shared without their consent.

Recent surveys illustrate this point. Just this week, researchers at the Annenberg School and UC Berkeley released a survey in which over 80% of consumers stated that they would not want to receive online ads based on data gathered about their online activities across multiple websites.[10] A 2007 survey found that 45 percent of consumers believe that online tracking should be prohibited, and another 47 percent would allow such tracking, but only with some form of consumer control.[11] These surveys underscore the fundamental value that consumers place on privacy in itself. Thus, the behavioral advertising principles we have developed are not limited to practices that may cause economic or other concrete harm; rather, they recognize what these survey data confirm – that many consumers simply do not want their information tracked and many want the power to exercise control over when tracking occurs and the uses to which the data collected can be put.[12]

My recent letter to Google further illustrates the point. Due to its plans to digitize millions of books, consumers may now be able to read anything from John Steinbeck to John

---

[10] *See* Turow, King, Hoofnagle, Bleakley, and Hennessy, "Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It," (September 2009), *available at* http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

[11] *See* George R. Milne, "Information Exchange Expectations of Consumers, Marketing 15 Managers and Direct Marketers," University of Massachusetts Amherst (presented on Nov. 1, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/presentations/3gmilne.pdf.

[12] *See* Federal Trade Commission, Self-Regulatory Principles for Online Behavioral Advertising, February 2009, http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf.

Grisham online. But in certain cases, they may not want anyone to know their reading habits. To address this issue, I requested that Google disclose how it will use the personal information it collects when it offers books online and delivers targeted advertising to consumers. I further called upon Google to commit to complying with the FTC's self-regulatory principles for online behavioral advertising.[13]

The Commission also has recognized privacy as an important value in the health area. Recently, the Commission entered into a consent agreement with CVS Caremark Corporation, requiring the company to properly dispose of sensitive prescription information.[14] As with the Google books example, I may or may not be harmed if people know that I take Percocet or Prednisone, but I still may want to keep that information private. Similarly, last month, the Commission's health breach notification rule went into effect. It requires certain web-based businesses to notify consumers about any breach of their individually identifiable health information, without regard to whether the breach caused tangible economic or other harm.[15] The lesson we have learned from all of our work is this – privacy is simply an important value that we must work to protect. We will keep this lesson in mind as we move forward on our project to explore new privacy frameworks.

D. Lesson 4: Don't throw out the good with the bad.

The fourth lesson is that we shouldn't throw out the good out with the bad. In this

---

[13] *See* Letter from David Vladeck to Jane Horvath Concerning the Google Books Project http://www.ftc.gov/os/closings/090903horvathletter.pdf.

[14] *See In the Matter of CVS Caremark Corporation*, FTC Docket No. C-4259 (Jun. 18, 2009).

[15] *See* www.ftc.gov/healthbreach.

context, the imperative to protect privacy should not deprive consumers of the benefits associated with information collection. For example, if we were to ban behavioral advertising altogether, consumers would not have access to much of the free online content they have come to expect.

When it comes to technology, we can't put the genie back in the bottle; nor would we want to. I touched on this subject at the beginning of my remarks – let's not go back to the days of encyclopedia research. Some of you can't imagine a world without the Internet, cell phones, or Blackberries, all of which permit the ubiquitous exchange of personal information. If we had been driven purely by fears of consumer privacy, none of these technologies would have flourished. Our policies must not discourage tomorrow's innovators.

E. Lesson 5: Keep up with the Joneses (or the Gates' and the Jobs')

Lesson 5 is that it really does pay to keep up with the online version of the proverbial Joneses; in this case, our policies need to keep up with the Gates' and the Jobs'. Put simply, our policies need to keep pace with rapidly-developing technology. This is a little different from Lesson 4, where I talked about the need to encourage new business models and technologies that benefit consumers. In addition to ensuring that our policies don't stifle innovation, we should ensure that the policies themselves do not become outdated.

Our behavioral advertising report contains an important example. It recognized that we should not protect the privacy of information only when it is associated with a particular name – the question of what is "personally identifiable" information has changed as technology has evolved. With the development of new and more sophisticated technologies, it is easier to identify an individual consumer based on information traditionally considered to be non-personally identifiable. For instance, although industry has traditionally considered most IP

addresses to be non-personally identifiable, it soon may be possible to link more IP addresses to specific individuals. In addition, even if certain items of information are anonymous by themselves, they can become identifiable when combined with other information. Professor LaTanya Sweeney from Carnegie Mellon University has estimated that 87% of the U.S. population can be uniquely identified if only a date of birth, gender and five-digit zip code are known.[16] Thus, we can't just focus our policies on protecting people's names, Social Security numbers, and financial account numbers – we have to think about how technology has evolved in determining what sets of data to protect. In other words, our policies must translate to current circumstances – we can't sell 8-track policies in an iPod world.

IV. Conclusion

In conclusion, though the lessons are simple, the issues are complex ones that will affect businesses and consumers in every sector of the economy. If we do not proceed carefully, we risk compromising consumers' privacy, imposing undue costs on businesses, and depriving consumers of the benefits they have come to expect. To maximize the chances of getting it right, the Commission believes that it would benefit significantly from broad-based discussion and input from practitioners, academics, consumer advocates, international experts, state government representatives, technologists, and others.

This brings me back to the themes I opened with – we must promote transparency and accountability from everyone. The government is no exception. We are hosting these roundtables publicly so that our policymaking can be transparent. And we truly believe that a spirited public debate on the issues will help us to get the policy right, because we know we'll be

[16]Hamblen, Matthew, "Privacy Algorithms," ComputerWorld (October 14, 2002).

held accountable to you. We look forward to working with you, and we especially look forward to seeing you in December.