Federal Trade Commission

"The Role of the FTC in Consumer Privacy Protection"
International Association of Privacy Professionals
Practical Privacy Series
Washington, DC

Remarks of David Vladeck[1]
Director FTC Bureau of Consumer Protection,
December 8, 2009

Good morning. I am so pleased to see this distinguished group gathered to discuss the role of the FTC in protecting consumer privacy. As you know, privacy is a cornerstone of our consumer protection agenda, and I would like to set the stage for today's discussion by talking about the past, present, and future of the FTC's work in consumer privacy. I will begin with the past: the FTC has been active in this area for a long time, and I will provide a brief overview of how we became involved in consumer privacy issues in the evolving online marketplace. Then the present: we are extremely busy on the enforcement and policy fronts. Some of the issues we are grappling with – such as improving transparency and control for consumers – are familiar. Others – such as our focus on health privacy – are evolving. I will talk about some of our recent activities in these and other areas. Finally, the future: the FTC has begun a public dialogue about existing regulatory and self-regulatory models and how effective they are at protecting consumer

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

privacy in a rapidly changing marketplace. We held the first of our "Exploring Privacy" roundtables yesterday, and I will close with an overview of next steps in that process.

The Past: The FTC's History of Consumer Privacy Protection

Today's discussion will explore the role of the FTC in consumer privacy protection. I'll begin with a very brief overview of how we got here. In the mid-1990s, the Commission began examining online privacy issues in order to address developing consumer concerns about what information was being collected, how that information was being used, and whether that information was secure. As many of you may remember, the Commission's early work on privacy focused on the fair information principles – notice, choice, access, and security. These fair information principles were based on the important underlying concepts of transparency, accountability, consumer autonomy, and individual preference. To further adoption of these principles, the Commission held public workshops; examined website information practices and disclosures regarding the collection, use, and transfer of personal information; commented on self-regulatory efforts and technological developments intended to enhance consumer privacy; conducted surveys of online privacy policies; and issued reports to Congress on the subject.

During this period, the Commission also identified enforcement – the use of a reliable mechanism to sanction noncompliance with the fair information principles – as a critical ingredient in any governmental or self-regulatory program to ensure privacy online. Our commitment to strong enforcement has been a foundation of our privacy program from the beginning. For example, in February 1999, the Commission settled charges that GeoCities, one of the most visited websites at the time, had misrepresented the purposes for which it was collecting personal identifying information from both children and adults. And in 2000, the Commission challenged a website's attempts to *sell* personal customer information, despite its

promise that such information would never be disclosed to a third party. These cases demonstrated the Commission's commitment to the fair information principle of enforcement and to protecting consumers' online privacy as an integral part of its law enforcement mission.

In the early 2000s, the FTC shifted its focus away from the fair information principles approach and adopted a "harm-based approach" designed to target harmful uses of information, without requiring notice and choice for *all* uses of information. The new approach focused primarily on tangible harms, such as physical harm, economic harm in the form of identity theft or denial of credit, or unwarranted intrusions into people's daily lives. In addition, during this period, the Commission began addressing offline, as well as online, practices. Accordingly, the Commission's privacy agenda since 2001 has focused on such issues as: (1) combating identity theft; (2) encouraging companies to maintain data security; (3) protecting children's privacy; and (4) protecting consumers from unwarranted intrusions into their daily lives, including spam, spyware, and telemarketing. We have been very active on these issues – we have dozens of enforcement actions in these areas – as well as a strong record of outreach to consumers and businesses. We remain committed to addressing these consumer privacy harms, even as we reexamine existing privacy frameworks and identify new areas of concern to consumers.

Present: Current FTC Enforcement and Policy Priorities

Now, I would like to turn to the FTC's current enforcement and policy priorities in consumer privacy. Some of these priorities, such as improving transparency to consumers, have been central to our privacy agenda from the beginning. Others, such as health privacy, are newer areas of focus for us, but are priorities as well.

Transparency

Transparency has long been a core priority in the FTC's efforts to protect consumer

privacy. Although some of our early work focused on the use of online privacy statements to inform consumers about the collection and use of their information, more recently we, along with many others, have recognized the limitations of that approach.

A recent Commission enforcement action demonstrates the problems with lack of transparency of privacy practices. This June, Sears agreed to settle an FTC complaint alleging that the company 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, passwords, drug prescription records, video rental records, and library borrowing histories. Only at the end of 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. As this case demonstrates, without real transparency, consumers cannot make informed decisions about sharing their information.

In the context of online behavioral advertising, we have encouraged companies to design innovative ways – apart from privacy policies – to inject greater transparency in their interactions with consumers. For example, imagine that a consumer gets a targeted ad based on his or her search history. A company could provide 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 just-in-time disclosure is likely to be

far more effective than a discussion – even a clear one – that is buried within a lengthy privacy policy that the consumer has to hunt for, click on, and then read.

We are also working to promote transparency by addressing the problem of buried disclosures related to free credit reports. Recently, the FTC issued proposed amendments to the "Free Credit Report Rule" designed to prevent consumer confusion in advertisements for free credit reports. Under the Credit CARD Act of 2009, the FTC was directed to issue a rule to prevent deceptive marketing of "free credit reports." The Act requires that advertisements for "free credit reports" include prominent disclosures designed to prevent consumers from confusing these so-called "free" offers with the federally mandated free annual credit reports. To promote transparency the proposed amendments require Internet sites offering free credit reports to direct consumers to a landing page that would contain the required disclosure and no other text. It would say – "This is not the free credit report required by Federal law. To get your free report, visit www.AnnualCreditReport.com or call" a specified toll-free number. The comment period on this proposal closed yesterday, and we expect to issue a final rule in February 2010.

Our concern about the adequacy of current notices has not been confined to the online world. We recently announced, along with seven other regulatory agencies, the release of a final model privacy notice form that will make it easier for consumers to understand how financial institutions collect and share information about them. The Gramm-Leach-Bliley Act required financial institutions to send notices, beginning on July 1, 2001, that inform customers of their privacy practices and provide an opportunity to opt out of having their personal information shared with unaffiliated third parties. In implementing this requirement, financial institutions sent privacy notices that were extremely long and complex legal documents, turgidly written,

with buried disclosures that consumers often did not find. As a result, they could not make a meaningful decision to opt out of particular practices. In addition, the notices were difficult to compare, even among financial institutions with identical privacy practices. As part of an effort to streamline those privacy notices, we worked with our sister agencies to conduct extensive consumer research and testing to develop a model notice that is useable and meaningful for consumers.

Together, these initiatives demonstrate the FTC's continued commitment to increasing transparency for consumers in a variety of contexts, including online and offline transactions, so that they will have the tools necessary to make meaningful, informed choices.

Health privacy

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 information, including prescription information. In some senses, this was a traditional FTC data security case highlighting issues such as the importance of secure disposal and adequate employee training and oversight. In other senses, it was a groundbreaking case. It was the first time the Commission had challenged the reasonableness of security measures to protect *employee* data, in addition to customer data. Moreover, the CVS case highlights our growing interest in the area of health privacy, where consumers may suffer harms not addressed by the Commission's traditional harm-based model. For example, a consumer may or may not be harmed economically if people know that he takes Vicodin or Viagra, but he still may reasonably expect that that information will be kept private.

Similarly, the Commission recently issued a final health breach notification rule. The rule requires certain web-based businesses to notify consumers about any breach of their

individually identifiable health information, without requiring an analysis of whether the breach caused tangible economic or other harm. The FTC will begin enforcement of the rule in February 2010.

Cross-border data flows

Another priority for the FTC is cross-border privacy issues and international enforcement cooperation. Our efforts in this area are gaining greater importance in light of ubiquitous cross-border data flows, cloud computing, and on-demand data processing that takes place across national borders. To protect consumers in this rapidly changing environment, we are engaged in various policy initiatives to protect consumer privacy while facilitating cross-border data flows. One is the U.S.-EU Safe Harbor Framework, which gives U.S. companies a method for transferring personal data outside Europe consistent with U.S. and European law. The FTC serves as a backstop enforcement authority for this framework. In addition, we are engaged in the APEC initiative to establish cross-border privacy rules, which aim at providing a self-regulatory mechanism for companies to transfer data throughout the APEC region under a consistent set of rules.

We have also recently announced a number of enforcement actions in this area. The first was against a California-based company that the FTC alleges deceptively sold electronics to hundreds of British consumers. Using two dot-UK Web addresses, the company purportedly tricked consumers into believing that they were doing business with a UK company. Consumers were charged unexpected import duties, received invalid warranties, and were charged draconian fees if they returned the merchandise, which was in some cases unusable. The case is notable because it was brought against a U.S. company exclusively doing business abroad and also because it highlights our commitment to working with our international law enforcement

partners. In addition, the complaint contained an allegation that the company deceptively claimed to be a member of the U.S.-EU Safe Harbor Framework.

We also announced six enforcement actions against companies that were claiming to hold current self-certifications to the Safe Harbor Framework, when in fact they did not. Our consent agreements with these companies prohibit them from misrepresenting their participation in any privacy, security or other compliance program, among other provisions. If the companies engage in such misrepresentations in the future, they could be subject to civil penalties for order violations. These cases, along with our ongoing policy initiatives, demonstrate our commitment to protecting consumer privacy as information travels across borders.

Emerging Technologies and Business Models

Consistent with our long-standing practice in the consumer privacy area, the FTC continues to examine emerging business models and their impact on consumers. We are examining a broad range of technologies and business models – online behavioral advertising, cloud computing, social networking services, mobile and location-based services, and peer-to-peer file sharing. We have already identified some key areas of concern for consumers. For example, as consumers rely more and more on mobile computing devices (with their small screens), how can businesses be transparent about their data collection and use practices? And as responsibility for data protection becomes more diffuse – as in the case of cloud computing, where invisible service providers may remotely store and process data – who is responsible for safeguarding it? 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. Finally, similar challenges arise in the area of P2P file sharing. Consumers who download P2P software to share music

files, knowing that their music files are accessible to others, may not be aware that the software can give people access to *all* of the personal data from their computers.

My recent letter to Google regarding the Google Books settlement tries to address some of the issues raised by emerging business models. Due to its plans to digitize millions of books, consumers may now be able to read anything from the Koran to the Kama Sutra online. But 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, which emphasize, among other things, the core values of transparency and consumer control.

Future: Examining Privacy Frameworks

And now, the future. We have learned that existing privacy frameworks have their drawbacks. The notice and choice model puts the burden on the consumer to read and understand lengthy, complicated privacy policies. The harm-based model recognizes only a narrow set of harms, but, as some of the examples I have mentioned demonstrate, privacy is an important value in itself. The FTC is engaged in a public dialogue to re-examine the effectiveness of existing frameworks to protect consumer privacy through a series of roundtables, the first of which took place yesterday.

Let me share some observations from yesterday's roundtable. We began the day discussing the wide variety of ways by which consumer information brings benefits – through subsidizing the Internet and more relevant advertising – as well as the risks posed by the possible misuse of that information. We heard experts confirm what we have sensed – that consumers do not really understand data collection and are largely unaware that there may be companies

collecting and analyzing their data for other companies to use, particularly for targeted advertising. We discussed in greater detail the collection and use of data in two specific contexts – behavioral advertising and the information broker industry – that remain highly visible issues in consumer privacy. Finally, we heard discussions about various approaches to managing the privacy and security of consumer information – the fair information principles, the harm-based approach, sector-specific regulation, and self-regulation.

We will continue these discussions and address new topics at the next roundtable, which will take place on January 28 in Berkeley, California. There, we plan to have a broad discussion of the impact of technology on privacy – looking at technology as a way of promoting consumer privacy, as well as a tool for undermining it in some cases. The third and final roundtable will take place in mid-March in Washington, D.C., and we look forward to continuing to work with stakeholders throughout this process and beyond. The role of the FTC in this space is an important one, but it is critical that we partner with a broad range of stakeholders – practitioners, academics, consumer advocates, industry representatives, international experts, technologists, and others – as we continue our mission of protecting consumer privacy in a complex and changing environment. Thank you.