RECENT PRIVACY DEVELOPMENTS AT THE FTC

Remarks before the
Twenty-Ninth Asia Pacific Privacy Authorities Forum

Seoul
June 19, 2008

William Blumenthal [*]
General Counsel
Federal Trade Commission
Washington, D.C.

I would like to thank the Asia Pacific Privacy Authorities for inviting me to appear before this Forum. Many of the government representatives here today have worked over the years in other settings with my FTC colleagues Hugh Stevenson, Stacy Feuer, Markus Heyder, and others. I bring their greetings. We are all delighted that my presence here in Seoul at the OECD's Internet Ministerial has afforded the opportunity to participate today in this related event and to join other agencies in providing a "jurisdiction report."

This morning I will describe several recent developments in the FTC's privacy work, beginning with two enforcement actions arising from failures by legitimate businesses adequately to protect sensitive personal data. I will then turn briefly to the FTC's work on behavioral advertising principles and wrap up by discussing our involvement in the cross-border privacy rules under development within the Asia-Pacific Economic Cooperation organization.

First a bit of background: For any of you unfamiliar with the U.S. Federal Trade Commission, we are the only consumer protection agency of general jurisdiction in the United States. Protecting privacy is one of the agency's top priorities, and we do this through vigorous law enforcement, outreach to consumers and industry, and cooperation with our counterparts in state and federal agencies and foreign governments. Our main source of legal authority comes from our general consumer protection statute, the FTC Act, which prohibits unfair and deceptive business practices. We use our authority under this law in many of our privacy and data security enforcement actions. In addition to the FTC Act, we also enforce a number of laws dealing with the privacy and security of consumer information in specific contexts, such as financial privacy, credit reporting, telemarketing, and children's online privacy. In addition, the FTC is also responsible for

[*] These views are those of the speaker and do not necessarily represent the position of the Federal Trade Commission or of any individual Commissioner.

providing backstop enforcement for companies' public declarations to adhere to the privacy principles of the EU-U.S. Safe Harbor Framework relating to the transfer of consumer data from the EU to the U.S.

With that background, let me turn to the update on our recent privacy activities.

I. Recent Privacy and Data Security Enforcement

Since 2001 the FTC has brought twenty cases against businesses that misrepresented their privacy or data security practices or that failed to implement reasonable protections for consumer data. The FTC recently announced two settlements with companies that had suffered major data breaches involving the sensitive information of hundreds of thousands of consumers. We do not view a data breach alone as basis for liability. As to these particular breaches, however, FTC staff conducted thorough investigations and found that the breaches caused harm to consumers as a result of the companies' failure to provide reasonable and appropriate security for sensitive data. Together with our other cases in this area, these two enforcement actions represent the FTC's continued emphasis on vigorous enforcement of U.S. privacy laws.

A. TJX

The first breach involved TJX, a discount retailer with more than 2,500 clothing stores nationwide. The FTC alleged that TJX had failed to use reasonable and appropriate security measures to prevent unauthorized access to consumers' personal information, including credit and debit card information on its computer networks. The company's alleged security failures included, among other things, (1) storing and transmitting personal data in clear text, (2) failing to limit wireless access to its network, and (3) failing to require network administrators and others to use strong passwords. In our view these vulnerabilities, taken together, constituted a failure to provide reasonable and appropriate security for sensitive data, and they caused or were likely to cause substantial harm to consumers by putting their sensitive information at risk. An intruder had exploited these security vulnerabilities and obtained tens of millions of credit and debit payment cards that consumers used at TJX's stores, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. Banks have claimed that tens of millions of dollars in fraudulent charges have been made on the cards, and millions of cards have been cancelled and reissued. TJX and the FTC entered into a settlement under which TJX agreed to implement and maintain a comprehensive information security program and to obtain audits by independent third-party security professionals every other year for a period of twenty years.

B. Reed Elsevier and Seisint

Similarly, in our enforcement action against Reed Elsevier (REI) and Seisint, the FTC alleged that the companies failed to implement reasonable security for the consumer information that they collected and stored in their databases. The companies served as

data brokers and, in that capacity, maintained information about millions of consumers, including names, current and prior addresses, dates of birth, driver license numbers, and social security numbers. They sold this information to their customers, who in turn used the information to locate assets, authenticate identities, and verify credentials. REI and Seisint relied on user identifications and passwords to control their customers' access to the consumer information in the databases.

Among other security failures, the FTC alleged, REI and Seisint had failed to require their customers to use strong passwords to access their databases, putting consumer information at risk. As in the TJX matter, the FTC alleged that the companies failed to provide reasonable and appropriate security for sensitive data, which caused or was likely to cause substantial harm to consumers by putting their sensitive information at risk. The security failures led to a data breach: Identity thieves were able to use customers' usernames and passwords to obtain access to sensitive information about at least 316,000 consumers. The thieves then used the information to commit credit card fraud and open new accounts.

REI and Seisint and the FTC entered into a settlement under which the companies agreed to establish and maintain a comprehensive information security program to protect personal information and to obtain audits by independent third party security professionals every other year for a period of twenty years. Together with our other privacy and data security enforcement actions, these cases send a strong message to industry that they must implement reasonable measures to protect the privacy of consumer data.

II. BEHAVIORAL ADVERTISING PRINCIPLES

Now I would like to turn to the FTC staff's recent work on Behavioral Advertising Principles. When I use the term "behavioral advertising," I am referring to the practice of tracking consumers' activities online in order to target advertising more precisely to consumers' specific interests.

Last year, the FTC convened a two-day public workshop to explore the privacy issues associated with behavioral advertising. Participants discussed the benefits of online advertising, including its support for free content and its ability to personalize advertisements in a way that many consumers value. But participants also expressed concern that behavioral advertising is largely unknown to consumers and that the data collected for behavioral advertising could fall into the wrong hands or be used for unanticipated purposes.

To respond to these concerns, the Commission staff has issued a set of draft principles that are intended to encourage more effective industry self-regulation of behavioral advertising practices. These self-regulatory principles include the following:

Transparency and consumer control – Every website where data are collected for behavioral advertising should post a clear, concise, consumer-friendly, and prominent statement that data are being collected to provide tailored advertising and that consumers can choose whether to have their data collected for that purpose.

Reasonable security and limited data retention – Any company that collects or stores consumer data for behavioral advertising should provide reasonable security for the data and should retain data only as long as necessary to fulfill a legitimate business or law enforcement need.

Affirmative express consent for material changes to existing privacy promises – Companies should obtain consent from affected consumers before using data in a manner materially different from promises the company made when it collected the data.

Affirmative express consent to use sensitive data for behavioral advertising – Companies should obtain consent before collecting and using sensitive data, such as information about health conditions, sexual orientation, or children's activities online, for behavioral advertising.

Call for additional information – The FTC sought more information on whether the use of sensitive data should be prohibited altogether and whether the principles should address the use of tracking data for purposes other than behavioral advertising.

The FTC sought public comment on the principles, and the comment period closed on April 11. We received 62 comments from a wide range of sources – companies that engage in behavioral advertising, consumer advocates, trade associations, technologists, and others. The comments are available on the FTC website at http://www.ftc.gov/os/comments/behavioraladprinciples/index.shtm, and staff is reviewing them. After completing the review, I expect we will have more to say with the hope of spurring action on the part of industry and others to develop self-regulatory initiatives that are meaningful and effective for the public.

III. APEC CROSS-BORDER PRIVACY RULES

The last item I want to address this morning is our involvement in the APEC cross-border privacy rules project, a project that will be familiar to many of you. For those of you who have not been involved with the project, APEC cross-border privacy rules are one mechanism for implementing the APEC Privacy Framework. That Framework is intended to facilitate cross-border electronic commerce in the Asia-Pacific region, while at the same time ensuring privacy protections for consumer data across the range of legal systems and privacy regimes that exist throughout the region.

The Framework includes nine "high-level" Information Privacy Principles that apply to the personal information of individuals. APEC cross-border privacy rules are one way of translating these high-level privacy principles into operational rules for transferring and accessing consumer data across borders. To develop these rules, the members of the APEC Data Privacy Subgroup, including the FTC, have been actively engaged on an official APEC Privacy Pathfinder project. Most, if not all, of the privacy authorities in this room are participating in various Pathfinder working groups with the objective of developing and testing various aspects of a system of cross-border privacy rules, including substantive program requirements for participating businesses, procedures for certifying businesses as eligible to participate, and dispute resolution and enforcement mechanisms for ensuring compliance.

Ultimately, this system would allow participating global businesses to transfer consumer data across borders, supported by a coordinated enforcement network of participating private sector organizations, such as trustmarks, and government backstop law enforcement. One of the goals is to create enhanced uniformity and consistency, which in turn should yield efficiencies and cost savings. Likewise, the creation of more effective privacy law enforcement across borders should result in enhanced tools for protecting consumer privacy.

Perhaps the biggest challenge in creating this system will be to accommodate the differing approaches of domestic legal frameworks while ensuring enough compatibility to allow effective international cooperation. Different APEC economies have different ways to implement their piece of the cross-border rules network. For example, in the U.S., the approach will involve a combination of industry self-regulation and government backstop enforcement.

We are still in the project's development phase, and there is much more to learn, but the development of APEC cross-border privacy rules remains a priority for the FTC. We believe the project, if successful, may be instructive outside of APEC, particularly where countries with divergent legal and privacy systems attempt to protect the privacy interests of their consumers cooperatively and creatively and without creating unnecessary barriers to cross-border business.

CONCLUSION

The FTC's privacy work has many additional aspects, but this morning does not allow for a comprehensive review, so I hope my summary of three components will suffice. Let me conclude with this observation: The global, electronic nature of modern business brings new challenges in the area of privacy enforcement. We have to ensure that our policies, practices, and enforcement structures stay current. My colleagues at the FTC are committed to doing so, in cooperation with the authorities at today's Forum and with our other foreign counterparts.