Federal Trade Commission

Deborah Platt Majoras[1]
Chairman, Federal Trade Commission
The IAPP Privacy Summit
March 7, 2007

Building A Culture of Privacy and Security -- Together

I. Introduction

It is a great pleasure to speak to what I understand is "the largest gathering of privacy professionals in the world." In preparing to speak to you, I went to the IAPP web site to try to learn how your organization defines a privacy professional, and I discovered that the site has been sponsoring a challenge for IAPP members on this very topic. According to some of you, a "Privacy Pro" is: "a juggler, a diplomat, a guardian, an enforcer, a psychologist, and a genius"; "a bodyguard of your identity, protecting your personal information from thieves, busybodies, bullies, wanna-be big brothers"; "the new sheriff in town in today's Wild West"; "a traffic cop"; and "a mystic on the mountain of the corporate world."

I have no doubt that there are some days when you feel that you are expected to perform all of these roles. But the answer that struck me was one that described a privacy professional as someone "who lives on the edge of a sword," ensuring that his or her organization "safeguards its

[1] These remarks are my own and do not necessarily represent the views of the Commission or any other Commissioner.

customer information so as to maintain their trust," yet also "faces pressure from the marketing forces within the organization to release as much data as possible to generate revenue." Finding the right balance between the need to collect, use, and store information and the need to provide adequate privacy and security protection seems to me to be at the heart of being a privacy professional. This is a challenge for every privacy pro – indeed, for every organization.

However defined, it is encouraging to see that more and more organizations are recognizing the importance of protecting sensitive information. Together, our thinking in this area must continue to evolve. No longer is it good enough for information security to be raised as an afterthought. Rather, it must be considered organically as organizations plan how they will do business.

II. Protecting FTC Information

The FTC is no different in this regard, and to be effective in our work to secure sensitive consumer information, we must look inward as well as outward. Accordingly, we have instituted an extensive and active program to instill and support a culture of privacy and security throughout the agency. Recognizing that protecting privacy and security of our own information is not a one-time task or paper exercise, the FTC has had a Privacy Steering Committee in place for some time. Last September, I appointed Marc Groman to be the Chair of that 20-person Committee and the FTC's first Chief Privacy Officer. As our Chief Privacy Officer, Marc is responsible for overseeing the FTC's own internal privacy policies and procedures. Significantly, he reports directly to the FTC Chief of Staff so that issues can be brought to my attention as quickly and directly as possible.

In 2006, the Committee undertook a comprehensive and systematic review of our policies

for the collection, use, sharing, retention, storage, and disposal of FTC information, with a particular emphasis on the treatment of personally identifiable information (PII) and sensitive health information. The Committee then developed detailed FAQs that provide practical advice regarding situations that staff is likely to encounter when handling PII during agency activities and held open discussion forums for agency staff in order to answer questions about the policies and to provide staff with an opportunity to identify additional issues and concerns.

The Committee also took the lead this year in bringing the agency into compliance with new privacy guidelines that the Office of Management and Budget issued for all federal agencies. In 2007, the Committee will continue and expand efforts to protect the FTC's own information. For example, we are holding an intensive Privacy Week for our employees at the end of this month. We will also develop a formal incident response plan setting forth how the FTC should respond quickly and thoroughly to a data breach. The dedication and hard work of the Committee - our in-house privacy professionals - is critical to enhancing the privacy and security culture at the FTC.

In addition to improving the handling of our own information, the FTC has been a key player in efforts to improve privacy and security throughout the federal government. Last year, President Bush created an Identity Theft Task Force, which Attorney General Gonzalez and I co-chair. The Task Force includes 18 federal agencies that are working together to develop a strategic plan to enhance the effectiveness and efficiency of government efforts to deter, prevent, detect, investigate, and prosecute identity theft. The Task Force already has made interim recommendations, one of which recommended the development of government-wide guidance addressing whether and how to provide notice to individuals in the event of a government agency

data breach.[2]

III. The FTC's Mission: Protecting Consumers from Privacy and Security Risks

As the nation's consumer protection agency, our core mission remains to ensure the security of information that the private sector collects, uses, and stores. Our fundamental objective is to develop, advocate, and implement policies that allow consumers to obtain the enormous benefits of information communication technologies in the marketplace without exposing them to undue privacy and security risks. Just as your privacy and security plans must be multi-faceted in order to be effective, so too is our strategy.

A. Law Enforcement

We are first and foremost a law enforcement agency. If you are reading your IAPP "Daily Dashboards," then you know that the FTC has enforced aggressively its primary enabling statute, Section 5 of the FTC ACT, which prohibits deceptive or unfair practices, and special statutes related to privacy, including the Gramm-Leach Bliley Act, the CAN-SPAM Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the FCRA, FACTA, and COPPA, as well as rules that we have promulgated to implement these special statutes.

The FTC has used our full range of enforcement authority to protect consumers from undue data security risks. The Commission has brought 14 law enforcement actions against companies that have failed to take reasonable measures to keep consumer information secure. In bringing each case, our message has been the same: companies must maintain reasonable and appropriate measures to protect sensitive consumer information. This requirement is process-

---

[2] *See* FTC Press Release, *Identity Task Force Announces Interim Recommendations* (Sept. 19, 2006), *available at* http://www.ftc.gov/opa/2006/09/idtheft.htm.

oriented, rather than technology-oriented. Because risks, technologies, and other circumstances change over time, a specific technical standard carved in stone soon could become obsolete or could have unintended consequences for competition and consumers, like stifling innovation. Further, there is no one-size-fits-all data security plan. Indeed, a data security plan must be adapted to the size and nature of the business, the nature of the information involved, the tools available, and the security risks the business is likely to face.

I want to emphasize two key points about the 14 data security cases the FTC has brought to date. First, none of these cases was a close call – in each case, vulnerabilities were multiple and systematic, and simple, readily available, low cost, measures were available to prevent them. They include cases against companies that threw files containing consumer home loan applications into an unsecured dumpster; stored sensitive information in multiple files when there was no longer a business need to keep the information; failed to implement simple, low-cost, and readily available defenses to well known Web-based hacker attacks; stored sensitive consumer information in unencrypted files that could be easily accessed using commonly known user IDs and passwords; and failed to use readily available security measures to prevent unauthorized wireless connections to their networks. Second, the violation alleged in each of these cases was not the breach itself, but the failure to take reasonable precautions to try to prevent a breach. Our standard is not perfection; it is reasonableness. But I want to underscore that the FTC will enforce aggressively this standard to protect data security.

In addition to data security, we also focus on on-line security. At the FTC, we have made a long-term commitment to combating spam, having brought 89 law enforcement actions against 241 companies and individuals who engaged in deceptive and unfair practices in connection with

the distribution of spam, including 26 of which were filed after Congress enacted the CAN-SPAM Act and eight of which were filed in the past fiscal year. Still, we are aware of reports that, notwithstanding government and private sector efforts, the amount of spam being distributed has been increasing. And as if that is not grim enough news, recent experience suggests that spam is being used increasingly as a vehicle for more pernicious conduct, such as phishing, viruses, and spyware. While winning this battle seems elusive, we cannot give up and cede the people's Internet to thieves. We need to search out new strategies, and so later this year, the FTC will hold a public workshop to assess whether there have been changes in the prevalence and use of spam and, if so, its implications for consumer protection policy.

Spyware also is a major focus of FTC law enforcement activities to protect consumer privacy in an online environment. Spyware may cause a full range of consumer injury, from keystroke logger software that tracks all of a consumer's online activity, causing a significant risk of identity theft, to adware that forces a consumer to receive a substantial number of unwanted pop-up ads. The FTC has focused significant resources addressing spyware, bringing ten law enforcement actions during the past two years against spyware distributors. These actions have reaffirmed three key principles. First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures about software and its effects are not adequate, just as they have never been adequate in traditional areas of commerce. And third, if a distributor puts an unwanted program on a consumer's computer, he or she must be able to uninstall or disable it.

The Commission's most recent settlement with Direct Revenue,[3] a distributor of adware, illustrates these principles. According to the FTC's complaint, DirectRevenue, directly and through its affiliates, offered consumers free content and software, such as screen savers, games, and utilities, without disclosing adequately that downloading these items would result in the installation of adware. The installed adware monitored the online behavior of consumers and then used the results of this monitoring to display a substantial number of pop-up ads on their computers. Consumers who sought to uninstall the adware discovered that it was very difficult for them to identify, locate, and remove. Among other things, the FTC's complaint alleged that Direct Revenue used deception to induce the installation of the adware and that it was unfair for the company to make it unreasonably difficult to uninstall the adware. To resolve these complaint allegations, DirectRevenue has agreed to provide clear and prominent disclosures of what it is installing, obtain express consent prior to installation, clearly label its ads, provide a reasonable means of uninstalling software, and monitor its affiliates to assure that they (and their own affiliates) comply with the FTC's order. In addition, Direct Revenue has agreed to disgorge $1.5 million in ill-gotten gains to the U.S. Treasury.

A third online privacy priority for our agency has been protecting children from privacy risks. The FTC is working to protect children under age 13 on the Internet through law enforcement actions brought under COPPA. For instance, we recently brought a case alleging that Xanga.com, a social networking web site, violated the Act and the Rule by collecting and disclosing, without parental consent, personal information in connection with 1.7 million

---

[3] *In the Matter of DirectRevenue, LLC et al.*, FTC File No. 052-3131 (Feb. 16, 2007) (consent agreement accepted for public comment), *available at* http://www.ftc.gov/opa/2007/02/directrevenue.htm.

accounts that children had created, and the company agreed to pay a $1 million civil penalty to resolve these allegations.[4] Not only was this our first COPPA case involving a social networking Web site, but it also was the largest penalty that the agency has ever obtained in a COPPA case. The Commission recently submitted a report to Congress assessing the effectiveness of the Act and the Rule during their first five years.[5] In the report, we concluded that the Act and the Rule generally have been effective in protecting children without adversely affecting their ability to access information online, and, therefore, no changes in the law are necessary. The report also emphasized the continuing importance of business and consumer education and technological innovation, such as the development of age verification technologies. Most significantly, the FTC's report stressed that protecting children online in the future will require vigorous COPPA law enforcement, including applying the law to new types of sites and services, as well as increased civil penalties.

Our commitment to protecting privacy extends to the off-line world as well, as our recent law enforcement actions related to telephone records pretexting illustrate. Last spring, we filed five actions against entities that obtained consumer telephone records from pretexters and then marketed this information to others. The dangers from pretexting are grave; in one of our cases, Commission staff obtained evidence that in some circumstances, defendants sold such records to abusive spouses who were subject to court orders of protection and who had threatened

---

[4] *United States v. Xanga.com, Inc., et al.*, Civ Act. No. 06-CIV-6853 (SHS) (S.D.N.Y. Sept. 7, 2006) (consent decree filed), *available at* http://www.ftc.gov/opa/2006/09/xanga.htm.

[5] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* (Feb. 27, 2007), *available at* http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

consumers with physical harm.[6] We have entered into settlement agreements with two of the five entities, prohibiting them from obtaining, or soliciting others to obtain, telephone records and from making them available to third parties. In addition, last month we filed charges against alleged telephone record pretexters, and we have asked the court to stop the conduct and to order the defendants to give up their ill-gotten gains.[7]

B. Consumer and Business Education

While our law enforcement actions are critical because they provide relief to injured consumers and a deterrent to those who might otherwise violate the law, it would, of course, have been even better if consumers had not been injured in the first place. To that I say, "Educate, Educate, Educate." To help empower consumers to avoid harm, and to assist businesses in implementing necessary security measures, the FTC has conducted extensive consumer and business education programs related to privacy and security, often in partnership with public or private sector entities.

A good recent example is our nationwide identity theft education program, "Avoid ID

---

[6] *See* FTC Press Release, *FTC Seeks Halt to Sale of Consumers' Confidential Telephone Records* (May 3, 2006), *available at* http://www.ftc.gov/opa/2006/05/phonerecords.htm.

[7] *FTC v. Action Research Group, Inc. et al.*, Civ Act. No. 6:07-C-ORL-22JGG (Feb. 15, 2007) (complaint filed), *available at* http://www.ftc.gov/opa/2007/02/arg.htn. In a welcome effort to add greater teeth to telephone record pretexting law enforcement, Congress late last year passed the Telephone Records and Privacy Protection Act, which President Bush signed on January 12, 2007. The Act makes it a criminal offense to make a false statement to a telephone service provider to obtain confidential records. Because of the serious harms that telephone record pretexting may cause consumers, it will continue to be a focus of our law enforcement activities and will result in referrals in appropriate cases to the Department of Justice for criminal prosecution.

Theft: Deter, Detect, Defend."[8] Through this initiative, we not only distributed direct-to-consumer brochures with this message, but we also created identity theft training kits that employers, community groups, members of Congress and others have used to spread the word about preventing ID Theft. The brochures and kits have been very popular – to date we have distributed more than 1.5 million brochures and 40,000 kits. I hope that, as privacy professionals, every one of you has a kit. You can obtain one by going to the FTC's web site. Another example is our "OnGuard Online" campaign. OnGuard Online is an innovative multimedia website that we developed in partnership with other government agencies and the technology sector. OnGuard Online offers guidance for consumers about online safety and provides information on specific topics such as phishing, spyware, and spam. The site also features interactive quizzes, articles, and videos on a range of topics, as well as information about other resources that are available to help consumers navigate the world of cybersecurity. Since its unveiling in September 2005, OnGuardOnline has attracted more than 3 million visitors, and many organizations – private and public sector – are linking to the site.

Business education is equally critical. I am pleased to release here today our latest business education initiative related to security. Most companies have some information in their files - names, Social Security numbers, credit card numbers - that identifies its customers and employees. We heard from some businesses, particularly smaller businesses, that they were not sure what data security measures they should take to protect such sensitive information from falling into the wrong hands. We therefore developed a brochure that articulates five key steps

---

[8] *See* FTC Press Release, *FTC Launches Nationwide Id Theft Education Campaign* (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/ddd.htm.

that are part of a sound data security plan. A copy of this brochure has been placed on your chair.[9]

The five key steps the brochure identifies are: "Take Stock" "Scale Down" "Lock It" "Pitch It" and "Plan Ahead." It then provides more specific information about what businesses should consider as they go through each of these steps. The brochure obviously will not answer all data security questions, nor is it intended to. Nevertheless, we anticipate that it will prove to be a useful tool in alerting businesses to the importance of data security issues and give them a solid foundation how to address those issues. If you are having trouble getting top management at your organization to pay attention to security issues, you may want to drop a copy of this brochure on their desks (perhaps along with a press release on one of our law enforcement actions!).

3. Research and Policy Development

Of course, an exciting yet daunting challenge of privacy and security issues is that the costs and benefits of practices frequently need to be reassessed in response to other changes, such as technological innovation. At the FTC, we continually endeavor to refresh our knowledge so that the policies we and others establish are as current and well-informed as possible. For example, authenticating individuals has become a critical topic for privacy professionals as limitations in current authentication methods have created opportunities for identity thieves to open new accounts and use stolen identities. To learn more about new and emerging authentication processes and their potential role in preventing identity theft, we will hold a public

---

[9] *Available at* http://www.ftc.gov/infosecurity.

Identity Management Workshop on April 23rd and 24th.[10] I invite all of you to join us.

It is not enough, though, to just tackle the problems we are encountering today. One of the first lessons taught to junior officers in the 18th Century British Navy was to resist the temptation to look downward to the turbulent sea on which they were sailing. Instead, they learned that they needed to discipline themselves to look to the sky, including the stars, to set a proper course to reach their destination.

In charting our course for privacy and security policy, sometimes we, too, need to take a longer-term view. Last November, the FTC held our "Tech-ade" hearings.[11] During four days of hearings, the Commission heard from 100 tech experts, including Trevor Hughes of IAPP, about the prospects for technological innovation, its impact on consumers, and how the FTC could adapt its consumer protection policies in response over the next decade.

We intend to issue an FTC staff report this spring describing what we heard at the Tech-ade hearings, including what we learned about the likely privacy and security challenges of the next decade. Then in November, we will host a series of Town Hall meetings around the country to supplement and expand on some of the key topics discussed at the hearings. We plan to consider what we hear at these meetings as part of the FTC staff's own internal strategic planning process, after which we will announce a Technology Research and Policy Development Plan for 2008.

---

[10] *See* FTC Press Release, *FTC to Host Identity Authentication Workshop* (Feb. 21, 2007), *available at* http://www.ftc.gov/opa/2007/02/authentication.htm.

[11] *See* FTC Press Release, *Hearings Will Explore Emerging Technologies and Consumer Issues in the Next Decade* (July 26, 2006), *available at* http://www.ftc.gov/opa/2006/07/techade.htm.

IV. The Future of Privacy and Security at the FTC

For now though, certain things seem clear. Some new technologies, like sensor networks and radio frequency identification, are likely to result in the collection of even larger amounts of information about consumers and their activities. Other new information-related technologies and techniques, like artificial intelligence and behavioral targeting, are likely to require more and more detailed information about consumers and their activities. Technological advances in data storage, such as perpendicular storage, will allow massive amounts of data to be stored. In short, we almost certainly will collect, use, and store an unprecedented amount of information in the future, and this is likely to raise new privacy and security risks.

Moreover, this information – while more accessible and thus useful – will also be at greater risk given its mobility. Many new information communication technologies will be interconnected so that data will move to an even greater degree among devices and across the Internet. Such interconnections undoubtedly will provide enormous benefits that we will quickly come to take for granted, but it also will increase the points at which security may be breached, as well as the scope of harm if a breach does occur. And, of course, as data becomes increasingly mobile, it will flow even more naturally across national and other jurisdictional boundaries than it already does today.

Thus, we are increasing our efforts in the international arena. To help us work more closely with other jurisdictions, in December, Congress passed the U.S. SAFE WEB Act, which significantly enhances our ability to cooperate and coordinate with foreign law enforcement officials. We now have additional tools to work better with foreign law enforcers, and we will use these tools effectively to protect consumers.

In addition, we have a long-standing and productive relationship working with the OECD and, participating in its Working Party on Information Privacy and Security, and a strong partnership with the EU, participating last fall in the Article 29 Working Party's meeting on international transfers of personal data and meeting recently to discuss identity theft initiatives. In addition, we are working with APEC on privacy and security issues, with my colleague FTC Commissioner Pamela Jones-Harbour recently playing a key role in enhancing this valuable relationship. And we are increasing our joint efforts on cross-border fraud with long-time partners like Canada to include mutual assistance on privacy issues, as well as seeking to build new relationships with developing countries.

V. Conclusion

Privacy and security issues are dynamic and evolving. The FTC's core mission, however, remains constant - protecting consumers from harm. Privacy and security will remain at the top of our consumer protection agenda. I look forward to working together with privacy professionals on future privacy and security challenges. Thank you.