Federal Trade Commission

Remarks of Deborah Platt Majoras[1]
Chairman, Federal Trade Commission
Chamber of Commerce
Washington, DC
December 5, 2006

"Protecting Consumer Privacy in an Information Age"

I. Introduction

Good afternoon. I appreciate having the opportunity to talk to you about "The Future of Privacy." For more than a decade, protecting the privacy of American consumers has been a top priority at the Federal Trade Commission. Privacy, while always important, has become an issue of significant concern to consumers in an information age. The explosive growth of the Internet and the development of sophisticated computer systems and databases has made it easier than ever for companies to gather and use information about their customers. In addressing privacy concerns, however, it is important to keep in mind that these new information systems can have tremendous benefits for consumers, who can access customer service hotlines 24-hours-a-day, have easier access to credit, and enjoy many marketplace conveniences that they have come to expect. At the same time, if we do not protect sensitive information adequately, consumers can be harmed and lose confidence in the marketplace. The balance must be carefully struck: ask consumers if they care about privacy, and you will get a resounding "yes;" ask consumers if they will tolerate being inconvenienced, and you will get a resounding "no." This is our shared

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

challenge.

At the FTC, our approach to privacy is one that combines aggressive enforcement under existing consumer protection laws, constant evaluation of the adequacy of existing policies, self-regulation, and education. We also work with our international counterparts to protect privacy and maintain the free flow of information across borders. Efforts in each of these areas play an important role and, together, they create a framework that strives to achieve what we believe is at the core of consumer privacy: preventing consumer harm.

II. Identity Theft

Today, for consumers, identity theft has become one of their top privacy concerns. Identity theft, a crime that afflicts millions of Americans, costs consumers and businesses valuable time and precious dollars.[2] During this past week, a woman from Montana called our Consumer Response Center to report her recent discovery that an identity thief had opened more than 17 credit card and bank accounts in her name. The thief had rung up almost $150,000 in charges on those accounts, including multiple automobile loans. Another consumer from the Dallas area called last week to report her recent discovery that an identity thief had obtained a $300,000 home loan in her name more than five years ago. A third consumer from Santa Ana, California, just submitted her identity theft complaint over the Internet. She reports dealing with the theft of her identity since 1995, initially discovering six accounts that did not belong to her at the time she tried to purchase a new car. Since then, she discovered that the identity thief was able to obtain a Social Security card using the thief's name and address, but the consumer's social security number and credit history. All told, the thief opened 15 accounts, charged over $20,000, and caused the consumer to spend countless hours tracking and correcting the problem.

Although this crime costs our citizens and businesses billions of dollars each year, the

---

[2] A recent survey by the Ponemon Institute found that an average data breach costs a business about $4.8 million total and about $180 per lost customer record, a 30% increase from 2005.

greater damage may be the potential cost of consumers losing confidence in the marketplace in general, and in electronic commerce in particular. Such a loss in confidence is one we cannot afford.

So, what are we doing about it? Identity theft takes many forms and thus must be attacked on many fronts. Fully 50 percent of identity theft victims do not know the origin of the theft, while the other half typically can link their loss to a discrete event. Some identities have been stolen through low-tech methods, like stealing a wallet or "dumpster diving." Other thieves use technology, like hacking into an organization's computer system or using a credit card "skimming" device. And the method of theft used may determine the type of identity theft that results – the use of an existing account, which is most prevalent but potentially less harmful to consumers, or the opening of new accounts in a victim's name, a less-prevalent but potentially more damaging crime.

Our attack must incorporate more energy, more focus, more facets, and more creativity than the thieves are using. Both the public and private sectors must work in tandem with a sharp focus on three aspects: (1) deterrence, (2) victim recovery, and (3) apprehension and punishment. And we must keep in mind that our goal is to eradicate the crime, so as to maintain consumer confidence. Earlier this year, President Bush concluded that federal government resources directed at identity theft could be more effectively marshaled through a comprehensive and coordinated effort to combat ID theft. Accordingly, on May 10, 2006, the President established his Identity Theft Task Force, which Attorney General Gonzales chairs and I co-chair. In his Executive Order, the President directed the Task Force to submit to him a strategic plan for fighting ID theft. The 18 federal agencies that comprise the Task Force have been hard at work developing the plan.

In September, the Task Force issued a series of interim recommendations for actions that could be taken in the near-term to address the identity theft problem. As these interim recommendations recognize, aggressive law enforcement, improved security, enhanced victim

assistance, and more effective education are essential components in fighting identity theft. Recommendations already are being implemented. For example, members of the Task Force recently created a universal police report that makes it easier for identity theft victims to enter information about their experiences onto a common form, print the form, and submit it with their police report. It records the information in a format that can be entered into a common database for use by law enforcement. And the FTC is planning a Spring 2007 workshop to explore better methods for authenticating individuals.

In the next few days, we will post on the Web sites of the FTC, the Department of Justice, and other Task Force agencies a summary of possible recommendations to the President, with an invitation for interested parties to submit comments on those recommendations. Ultimately, we hope to deliver the strategic plan to the President early next year.

III. Data Security

Today, I am going to focus on the first goal of our identity theft efforts, deterrence. Deterrence begins with data security – keeping sensitive information out of the hands of wrongdoers. Security problems take many forms and present many challenges, but have one commonality – data thieves will exploit any available vulnerabilities to obtain sensitive personal information. Information is today's currency, and thieves know its value. Data security is important for every kind of organization – whether a company, government agency, or university; whether a mom-and-pop shop or a multinational corporation; whether a high-tech company or a low-tech business. It also is critical to every individual, each of whom must learn to better safeguard personal data.

And, as you well know, data security can no longer be viewed solely as a domestic issue. Like so many of the consumer protection issues that the FTC tackles, privacy and data security have "gone global." It no longer makes sense simply to refer to personal information being "here" or "there." The security of personal information no longer depends on the server room "in the back" being under lock and key. With the click of a mouse it can go to, or be accessed

from, just about anywhere. Protecting personal information now depends on the security practices of multiple organizations in multiple jurisdictions.

Public awareness of, and concern about, data security has reached new heights in recent months, as reports about the latest data breaches continue to hit the news with great regularity. Now, I certainly am aware that not all data breaches lead to identity theft and, in fact, that many lead to no harm whatsoever. And I am equally aware that not all identity theft results from breaches. But, there is no question that some breaches have led to fraud. Beyond that, the constant drumbeat about breaches is raising consumers' levels of stress and concern, which can contribute to reducing that all-important consumer confidence.[3]

Recent breaches have touched all sectors of the economy, and the nature of these breaches runs the gamut. A random sampling of incidents reported in the last few weeks reveals some different scenarios:

- The theft of two laptops containing health records of more than 7,000 patients of a cancer center;[4]
- The theft of three laptops containing payroll information for thousands of Scotland Yard employees;[5]
- The auction sale, over a seven-year period, of school district computers containing the birth dates, Social Security numbers, driver's license numbers and

---

[3] A survey of more than 1,000 victims of data security breaches found that nearly 20% of those victims terminated their relationship with the breached company. Another 40% stated that they might terminate their relationship. The range of total costs to the business was $226,000 to $22 million, making the average cost of a breach $4.8 million. *See* Vontu, Inc., "2006 Annual Study: Cost of a Data Breach" at 2, available at http://www.vontu.com/uploadedFiles/global/2006_Cost_of_Data_Breach_Report_V_2.pdf.

[4] Vijayan, Jaikumar, "Patient Data Exposed in Two Separate Security Breaches," ComputerWorld, November 29, 2006, available at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005518.

[5] "Laptop Thief Lands the Bank Details of 15,000 Policemen," thisislondon.co.uk, November 21, 2006, available at http://www.thisislondon.co.uk/news/article-23375377-details/Laptop+thief+lands+the+bank+details+of+15,000+policemen/article.do.

Department of Juvenile Justice records of approximately 100,000 students.[6]

We know that many organizations are investing the time, resources, and management attention necessary to protect personal data. But, "many" is not good enough – data security is the responsibility of *every* organization that maintains sensitive consumer information.

We also must remember that ensuring data security is not a static process or a one-time exercise. We cannot just issue a memo on security, check a box, and move on. Rather, as technologies and risks evolve and the marketplace changes, we need to reevaluate our data security programs and make improvements where appropriate.

And for those entities that have not yet "gotten the message,"[7] the FTC is using all legal tools at our disposal to send it loud and clear.

A. Guiding Legal Principles for the Private Sector

As you know, there is no single "data security" law, but rather a mosaic of federal and state laws that apply to certain entities or certain kinds of information. The Gramm-Leach-Bliley Act, for example, contains safeguards requirements for financial institutions;[8] the Fair Credit Reporting Act includes "know your customer" requirements for consumer reporting agencies;[9] and the Health Insurance Portability and Accountability Act, or HIPAA, protects the confidentiality and security of health information. In addition, the FTC has enforced the Federal

---

[6] "School District Sold Computers with Personal Information," MyrtleBeachOnline.com, November 27, 2006, available at http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/local/16109822.htm.

[7] One recent survey of U.S. small businesses, for example, found that over half of the companies had experienced a breach within the past 12 months, yet fully two-thirds of them still lacked an information security plan. Nearly 20% of these companies did not use virus scanning for email, and more than 60% did not use encryption to protect their wireless networks. This is not just a small business problem. A survey of multinational companies found that 86% of the firms had suffered a breach within the past three years, yet only about half of them had offered privacy awareness training for their employees. *See* Market Survey and Analysis Report, *Small Business Information Security Readiness*, Small Business Technology Institute (July 2005).

[8] 15 U.S.C. § 6801 *et seq.*

[9] 15 U.S.C. § 1681 *et seq.*

Trade Commission Act's proscription against unfair or deceptive practices in cases where a business made false or misleading claims about its security procedures, or where its failure to employ reasonable security procedures caused substantial consumer injury in the form of a data breach.[10]

Based on existing legal rules on data security, the FTC has developed and implemented a single, basic standard for data security: Companies should maintain reasonable and appropriate measures to protect sensitive consumer information. This "reasonableness" standard is explicitly required by the FTC's GLB Safeguards Rule[11] ("Safeguards Rule") and by the Fair Credit Reporting Act, and it has been applied by the Commission in bringing actions under Section 5 of the FTC Act.

The Safeguards Rule contemplates that reasonableness will depend on the sensitivity of the information at issue, the potential risks to that information, and the costs involved in avoiding those risks. Thus, a security plan should be adapted to the size and nature of the business, the nature of the information the business maintains, the security tools that are available, and the security risks the business is likely to face.[12] The Rule does not mandate specific technical requirements. This process-oriented approach recognizes that risks, technologies, and circumstances all change over time, and that a specific technical standard would soon be obsolete – and also might stifle innovation. Reasonableness does not mean perfection, of course; data security can be breached despite the best of security procedures. Thus, the fact that a company suffered a breach does not, in and of itself, establish that its practices were unreasonable, although it could be evidence of that fact. We believe this flexible

---

[10] 15 U.S.C. § 45.

[11] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, available at http://www.ftc.gov/ftc/legal.htm.

[12] For example, firms must prepare a written plan; designate an official with responsibility for the plan; identify, assess, and address foreseeable risks; monitor and evaluate the program for effectiveness; and adjust the plan as appropriate.

rule can serve as a model to guide all businesses in developing a data security program.

Of course, having a set of legal principles is not enough; they must be backed by vigorous enforcement. The FTC has brought 14 enforcement actions against businesses that have failed to provide reasonable data security. None of these cases has been a close call. 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.

Probably the best-known FTC enforcement action involving a security breach was our action against Choicepoint. Choicepoint, a data broker, inadvertently sold information on more than 160,000 customers to data thieves who used that information to open up new accounts and commit identity theft. The FTC alleged that ChoicePoint failed to use reasonable procedures to screen prospective subscribers. For example, the company allegedly approved as customers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby public commercial locations. The Commission obtained $10 million in civil penalties for the FCRA violations – the highest civil penalty ever levied in an FTC case – $5 million in consumer redress for identity theft victims, and significant injunctive provisions that require ChoicePoint to implement a variety of new data security measures.

The ChoicePoint case serves as a lesson in what can go wrong when you fail to do due diligence on the entities to which you disclose sensitive consumer information. But, I also mention this case to illustrate a different point – how companies can respond in a positive and

constructive way to "clean up their house" after they suffer a breach. ChoicePoint has instituted structural changes, such as creating the new position of chief privacy officer and centralizing its credentialing processes into a single department.[13] For example, ChoicePoint announced last year that it no longer would provide full Social Security numbers, birth dates, or other sensitive information to private investigators or other small customers. This decision reportedly cost the company an estimated $15 million to $20 million in lost business in 2005, but ChoicePoint executives believed that the risk to the company's reputation of pursuing this line of business outweighed the benefit. I am pleased that ChoicePoint has taken the lessons of its breach to heart and changed its operations to minimize the chances of such a breach in the future.

B. Pretexting

Because we lack criminal authority, as a general matter we do not target the perpetrators of identity theft crimes. In one area, however, the FTC has acted against "data thieves" – those who use pretexting to obtain and sell consumer data.

Pretexting, the practice of obtaining consumers' personal information under false pretenses, is a nice euphemism for simple fraud. And where there is fraud, the FTC is on the beat. Since 1999, we have brought numerous cases against pretexters of financial information, using our FTC Act authority, as well as the Gramm-Leach-Bliley Act's prohibition on this practice. More recently, we have turned our attention to an underground industry of consumer call records purveyors. Pretexters typically impersonate a customer to get his or her call records from a telephone carrier. In May, the FTC filed complaints in federal court against five Web-based entities that allegedly obtained consumers' confidential telephone records and sold them to anyone willing to pay a fee, alleging that these practices were unfair under the FTC Act. Of course, the practice of telephone pretexting has garnered national attention as a result of the Hewlett-Packard incident. As we learned in that case, call records can provide a window into the

[13] *See* Gary Rivlin, "Keeping Your Enemies Close," *New York Times* (Nov. 12, 2006) available at http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html

intimate details of a person's life. Even more disturbingly, they can facilitate stalking and worse.

C. Spyware

Another FTC enforcement priority that implicates privacy and data security is spyware. In its most pernicious form, spyware can include a keystroke logger to track all of a consumer's online activity, causing a significant risk of identity theft.

The Commission has brought nine enforcement actions involving spyware in the past two years. These actions have reaffirmed three key principles: First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures do not work, just as they have never worked in more traditional areas of commerce. And third, if a distributor puts a program on a consumer's computer that the consumer does not want, the consumer must be able to uninstall or disable it.

These principles are illustrated by the Commission's most recent spyware settlement, with Zango, Inc., formerly known as 180solutions. Zango provides advertising software programs, or adware, that monitor consumers' Internet use in order to display targeted pop-up ads. The consent order settles allegations that the company installed its advertising software programs on consumers' computers without adequate notice or consent. Zango's distributors frequently offered consumers free software without disclosing that downloading it would result in installation of Zango's adware. In other instances, Zango's third-party distributors exploited security vulnerabilities in Web browsers to install the adware via "drive-by" downloads. As a result, millions of consumers received pop-up ads without knowing why, and had their Internet use monitored without their knowledge. Moreover, the company deliberately made these adware programs difficult for consumers to identify, locate, and remove from their computers. The company used its adware to send billions of pop-up ads over several years. As part of the settlement, Zango agreed to disgorge $3 million in ill-gotten gains derived from its past actions, and it also agreed to injunctive provisions that will protect consumers in the future.

While we will not hesitate to use our full arsenal of legal tools to challenge inadequate

data-security practices, our goal is not to rack up prosecutions. It is to motivate the private sector to create a culture of security throughout their operations. In conjunction with our law enforcement, the FTC has published guidance for the business community on reducing threats to computer security and on complying with the Safeguards Rule.[14] The FTC also has issued a publication on managing data compromises.[15] I encourage you to look at these materials and to familiarize yourself with other resources that are available.

D. Public Sector Efforts to Improve Data Security

Your government, too, as a holder of extensive information on consumers, has more work to do to secure our data, and one important focus of the Identity Theft Task Force is ensuring that the federal government maintains high standards for data security.

As you probably know, all federal agencies, including the FTC, must comply with a comprehensive set of rules governing privacy and data security. The recent high-profile data security breaches at federal agencies, however, highlighted the fact that the federal government needs to do a better job. To that end, over the past six months, the Office of Management and Budget has directed every agency to implement new policy and procedural initiatives to better safeguard sensitive information. For example, each agency is required to encrypt all data on mobile computers and devices. And, drawing on the efforts of the Identity Theft Task Force, the government now has a plan for responding to data breaches that could pose a risk of identity theft.[16]

Social Security numbers often are the key to the most pernicious form of identity theft, when the thief opens new accounts in the consumer's name. Interim recommendations of the

---

[14] *See* Financial Institutions and Customer Information, Complying with the Safeguards Rule, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

[15] *See* Information Compromise and the Risk of Identity Theft: Guidance for Your Business, available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.pdf.

[16] *See* Memorandum from the Identity Theft Task Force, Identity Theft Related Data Security Breach Notification Guidance, September 19, 2006.

Task Force also included proposals to minimize or eliminate the unnecessary use of Social Security numbers. For example, the Task Force recommended that the Office of Personnel Management examine and reduce the collection and use of Social Security numbers in the human resources context. More broadly, the Task Force recommended that OPM issue guidance for agencies on ways to minimize or eliminate use of Social Security numbers by federal agencies, including on forms and systems, where they are unnecessary for an agency's operation or where an alternative, such as an employee number, can be used.

IV. Consumer Resources

While there is no guarantee that consumers can avoid identity theft, they are by no means powerless. They can and must take certain steps to avoid being victimized. In 1998, the Identity Theft Assumption and Deterrence Act ("the Identity Theft Act") assigned the FTC a unique role in combating identity theft and coordinating government efforts.[17] While we cannot prosecute the crime because we have only civil jurisdiction, we take consumer complaints and implement the Identity Theft Data Clearinghouse, a centralized database of victim complaints used by 1,300 law enforcement agencies; assist victims and consumers who wish not to be victims by providing information and education; and educate businesses on sound security practices.

Educating consumers is essential in the fight against identity theft. The FTC recently launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend." The message for consumers is that they can:

- DETER identity thieves by safeguarding their personal information;
- DETECT suspicious activity by routinely monitoring their financial accounts, billing statements, and credit reports; and
- And they should DEFEND against ID theft as soon as they suspect it. Quick action is

[17] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

essential.

One component of the campaign is a consumer education kit, which is aimed at helping organizations educate their employees, their customers, and their communities about how to minimize their risk. The kit includes a victim recovery guide, a training booklet, a guide to talking about identity theft, presentation slides, an easy-to-read brochure, and a 10-minute video.

The Deter, Detect, Defend campaign has been very popular – we have distributed more than 1.5 million brochures and 30,000 kits. And we have formed many partnerships to help us broaden our reach. Recently, for example, the National Association of Realtors, which has 1.2 million members, partnered with the FTC to educate homebuyers. NAR is distributing consumer education brochures and DVDs to realtors across the country, through its more than 1,400 local and state associations. All of the materials are available in English and in Spanish. I hope you will visit www.ftc.gov/idtheft to check them out, and use them in your education efforts.

The FTC also sponsors an innovative multimedia website, OnGuardOnline, designed to educate consumers about basic computer security.[18] The website offers guidance for 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 approximately 2.5 million visitors. Recently, several social networking sites featured OnGuard Online as a prominent link and have driven a good deal of traffic to our Web site. And for the second year in a row, Boeing is featuring OnGuardOnline materials in its internal security training.

Indeed, the FTC has recently collaborated with the Chamber of Commerce on consumer education issues. As part of a "Get Net Safe" initiative to promote online security, the Chamber and Microsoft co-sponsored panel discussions in 12 cities addressing how to stay safe online.

---

[18] *See* www.onguardonline.gov.

The OnGuard Online campaign is a featured part of this initiative.

V. Legislative Developments

As you know, Congress has been considering a variety of bills on data security. While none has been enacted to date, I expect that the new Congress will be revisiting this issue next year. I have testified several times on these issues, urging Congress to use caution in passing any new laws, so that in an effort to safeguard data we do not inhibit consumers' commercial transactions.

In our view, should Congress pass legislation, it should focus on imposing a reasonableness standard that would apply to all businesses that maintain sensitive consumer information. Most of the breach notification bills have included a "safeguards" requirement of this sort.

In addition, we have advised that Congress should consider a national data breach notification law that would require notice to consumers when their sensitive personal information has been breached in a way that creates a significant risk of identity theft.[19] Notice can help consumers prevent or mitigate harm resulting from a data breach by allowing them to take precautions. Notice alerts consumers whether they need to monitor their accounts more closely, close their accounts, or place fraud alerts on their credit reports. Notice also alerts consumer reporting agencies and law enforcement to the risk of fraud so that they can take appropriate actions to assist consumers in preventing identity theft.

In our view, however, notification makes sense only when it is useful to consumers, and not in situations involving remote or insignificant risks. Notifying consumers when risks are insignificant may cause them to spend time and money taking protective steps that are not necessary. Further, over time, excessive breach notification can overwhelm consumers, with the

---

[19] Prepared Statement of the Federal Trade Commission Before the Senate Committee on Commerce, Science, and Transportation, *Data Breaches and Identity Theft* (June 16, 2005) available at http://www.ftc.gov/os/2005/06/050616databreaches.pdf

result that they start ignoring such notification. Accordingly, breach notice legislation should include a risk-based trigger.

VI. Technology Developments

Of course, it is not enough to actively confront the privacy risks of today. We also must seek to anticipate and understand the risks of tomorrow, and then develop sound policies to address these new risks. In an effort to better understand the implications of technology changes on privacy and consumer protection, last month the FTC convened public hearings, which we dubbed "Protecting Consumers in the Next Tech-ade."[20] During the "Tech-ade" hearings, we heard from more than 100 of the best and the brightest in the tech world about the new technologies on the horizon and their potential effect on consumers.

Panelists raised privacy and data security issues, including during the discussions of, among other things, a range of payment devices and systems, such as on-line banking, contact-less devices, mobile telephone payments, and smart cards.

One data security issue discussed at the Tech-ade hearings aptly illustrates the potential benefits and risks of new technologies. Panelists at Tech-ade presented information about advances in biometrics used to authenticate a person's identity for data-access or other purposes.[21] Biometrics links information to a particular individual, unlike passwords that must be carried or remembered, and that could be used by others. While we were familiar with the use of some types of biometrics, like fingerprints and retinal scans, we learned for example, that each person apparently gives off a unique odor that in the future may be used for authentication.

While advances in biometrics may be a boon to authentication, nonetheless some panelists said that the use of biometrics for authentication creates risks as well. If a hacker gains access to a database and steals an employee's password to engage in identity theft, the employee can call

---

[20] For further information about this event, see http://www.ftc.gov/bcp/workshops/techade/who.html.

[21] Authentication involves comparing information that an individual provides (such as a password or fingerprints) with stored information to determine whether there is a match.

their help desk to immediately prevent the hacker's ability to use the old password. In contrast, if a hacker gains access to a database and steals the employee's fingerprint records to engage in identity theft, the solution may not be quite so simple. In short, although biometrics may improve authentication, to improve data security overall it is critical that stored biometric data – a "honeypot" for identity thieves – be kept secure.

As I mentioned earlier, the FTC and other Task Force members will explore consumer authentication issues in more depth at a workshop we will hold in spring 2007. To the extent we cannot keep all sensitive information out of the hands of wrongdoers, we can make it harder for them to use it to open new accounts by bolstering procedures for verifying that applicants really are who they say they are. Many of you are grappling with authentication issues, and we hope that our workshop will help spur the development of more-effective techniques or processes.

Learning about new technologies at hearings and workshops is critical, but we need to use what we learn to develop and foster policies that will better protect consumers. To kick off a government dialogue on the technology developments of the next decade, at the end of the Tech-Ade hearings, nearly 200 government officials, including approximately 25 from other countries, spent a day in private discussions at the FTC. We discussed the array of innovations that may be in our future, their implications for consumer protection policy, and how we can work together better to protect consumers. The FTC will issue a report on the Tech-ade hearings next year, discussing how we intend to move forward to address the consumer protection challenges of the future.

VII. Conclusion

Issues of privacy and data security are dynamic and evolving. Governments are not generally known for being on the "cutting edge," but we must emerge from the cloak of bureaucracy to keep up with the pace of technology. Not only must we deploy our resources to address current challenges, but we must anticipate future challenges. I look forward to working with you to learn about and address these challenges in the privacy area.