"Respecting the Individual: Privacy Frameworks for the 21st Century"

Remarks by Commissioner Pamela Jones Harbour
Before the International Association of Privacy Professionals
National Summit[1]

Washington, DC
March 10, 2006

I. INTRODUCTION

Good afternoon. I am delighted to be here today to speak with you about privacy. As a courtesy to my colleagues on the Commission, I will begin with the usual disclaimer: the views I express here are my own, and are not necessarily those of the Federal Trade Commission or any other individual Commissioner.

During this summit, you have heard from some of the leading practitioners and scholars in the privacy arena. I am pleased to be a part of this important discussion. Today, I will address some recent privacy-related activities at the FTC. I will then offer my own thoughts about privacy and privacy principles, and I will end with some suggestions for the future.

II. RECENT ACTIVITIES AT THE FEDERAL TRADE COMMISSION

Over the past year, as most of you know, the FTC has been active in privacy enforcement. As I am sure you are aware, the Commission levied its largest civil penalty to date against ChoicePoint. The company will pay $10 million in civil penalties and $5 million in consumer redress to settle charges that its security and

record-handling procedures violated the FTC Act and the Fair Credit Reporting Act.[2] Specifically, the Commission alleged that ChoicePoint furnished consumers' credit reports to subscribers who did not have a permissible purpose to obtain them, and failed to maintain reasonable procedures to verify subscribers' identities and permissible purposes to use the information.[3] In addition to civil penalties and consumer redress, the settlement includes strong injunctive relief. ChoicePoint must establish and maintain a comprehensive information security program, and the company will be required to undergo audits by an independent third-party security professional every other year for the next 20 years.[4]

Last year, the Commission also entered into consent orders with BJ's Warehouse and DSW Inc.[5] The Commission did not obtain civil penalties in those cases because there were no violations of any of the Commission's trade regulation rules or any statutes specifically authorizing civil penalties. In both of these cases, the Commission used its authority under the FTC Act to stop unfair practices. The Commission alleged that the failure to take appropriate, reasonable security measures to protect the sensitive information of thousands of customers was an unfair practice that violated federal law. Like ChoicePoint, both companies agreed to implement a comprehensive information security program and to undergo audits by an independent third party security professional every other year for 20 years.[6]

I hope that these settlements will send a strong message to industry: companies will be held accountable for providing the care that consumers reasonably expect in handling their sensitive personal information.

DIRECTV was another civil penalty case resulting in high monetary fines for its violations of consumers' privacy. DIRECTV paid $5.3 million to settle FTC charges that it, and telemarketers calling on its behalf, contacted consumers on the National Do Not Call Registry and abandoned calls to consumers, leaving them with dead air. [7] Again, the FTC also obtained strong injunctive relief. DIRECTV must terminate any marketer that it knows (or should know) is making cold calls to consumers without express, written authorization from DIRECTV. The order also imposes extensive monitoring requirements on DIRECTV, requiring that the company oversee marketers selling its goods or services.[8]

The Commission also obtained significant civil penalties or disgorgement in other cases involving violations of the Do-Not-Call Rule or CAN-SPAM Act.[9] In addition, we have brought a number of law enforcement actions challenging the secret installation of spyware and adware on consumers' computers.[10] The Commission also challenged false claims about computer spyware and the products that supposedly remove it.[11]

I am very proud of the Agency's enforcement work over the past year.

To supplement and expand upon this critical enforcement activity, we have produced reports summarizing the issues surrounding spyware and radio frequency identification.[12] Staying on top of rapidly-changing technology is an important part of the FTC's work. In fact, the Commission recently launched its new Division of Privacy and Identity Protection in the Bureau of Consumer Protection, in order to more fully dedicate critical resources to this important area. Finally, last year, all five members of the Commission testified before the Senate Commerce Committee concerning information privacy, especially data breaches by data brokers and other companies.

III. PRIVACY PRINCIPLES

A. Stepping Back to Recollect Principles

Sometimes, as law enforcers, we are so busy dealing with problems caused by invasions of privacy – data breaches, pretexting, spam, Do-Not-Call violations, spyware, adware, violations of the FCRA – that it is difficult to step back and remind ourselves of the foundational principles upon which our privacy laws *should* be based. I appreciate the opportunity to share, with you today, my conception of those principles.

B. Patchwork of Laws to Deal with Specific Problems

As you are all aware, the United States has a sectoral approach – a number of different laws dealing with different aspects of personal privacy.[13] Such laws were enacted at different points in our history, and often were intended to deal with industry-specific or case-specific problems. Most of these laws afford consumers important privacy protections. But some commentators have argued that some of these laws actually may have decreased consumers' privacy rights, because they preempted state statutory or tort laws that were more forceful.[14]

C. Principles to Elucidate This Area

1. What Principles Should Be Used?

We work tremendously hard to enforce this complex patchwork of laws. As a result, we may not always step back – as we should – to address a more fundamental question: what overarching principles *should* be used to elucidate the area of information privacy? In 1928, Justice Louis Brandeis described "the right to be let alone" as "the most comprehensive of rights, and the right most valued by civilized men."[15] Today, we still have individuals who absolutely wish to be left alone. But we also have others – perhaps unimaginable to Justice Brandeis – who reveal their innermost thoughts and most private actions on national TV or on Internet blogs. How can we have a meaningful discussion of privacy when individuals have such

differing notions of what privacy *should* be? How can we reach a common understanding – one that can form the basis for a prevailing, sustainable national standard?

2. FIPS Can Elucidate This Area

In my remarks last June before the Senate Commerce Committee, I testified that the Fair Information Practice Principles could be used to elucidate this area.[16] I know that you are all familiar with these principles, which have rightly become the lodestar of many discussions about privacy. The 1973 Health Education and Welfare [HEW] Report described Fair Information Practices as follows:

- Personal data record-keeping systems must not be kept when their very existence is secret;
- An individual must be able to determine what information about oneself is in a record and how it is used;
- An individual must be able to prevent information provided about oneself for one purpose, from being used or made available for other purposes without the individual's consent;
- An individual must be able to correct or amend a record of identifiable information about oneself; and

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[17]

The OECD has built upon these Fair Information Practice Principles, and they are reflected in APEC's Principles as well.[18]

The FTC, in a report to Congress in 1998, described the Fair Information Practice Principles as "five core principles of privacy protection."[19] You may have heard my former colleagues describe these principles in shorthand, in years past, as (1) Notice, (2) Choice, (3) Access, and (4) Security.[20] Recently, the Commission has been concerned most often with the security of information. I believe that it is important to remember and recognize each of these principles, including the fifth one, enforcement.

The first of these principles is **notice**. In the 1998 report to Congress, the Commission stated:

> The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.[21]

I agree. Companies should make consumers aware of what they intend to do with a consumer's information. As I testified before Congress, companies should also provide notice to consumers if there is a risk of harm, such as identity theft, resulting from a data breach.[22] If there is a risk of harm, consumers will want to know. The consumer can then evaluate what, if any, steps should be taken to avoid that harm, if possible.

Adequate notice enables the second privacy principle, which is **choice**. Consumers should be able to choose with which businesses they wish to share information, and what information about themselves should be shared. Some individuals do not want to share any information with anyone at any time. Others will share all of it.

Most of us probably choose freely to share our name, address, and preferences for goods or services. Many of us would hesitate, however, if a company wanted to share the movies we watched; places we visit on the Internet or in person; or our detailed financial information. When consumers choose what information can be shared and with whom, there will be far fewer misunderstandings or annoyances. I would also imagine that when consumers deliberately choose to allow the sharing of their personal information, they will do so because they believe they are likely to receive some benefit for the use of their private information.

To categorize my approach to privacy, I would describe myself as a principled pragmatist. I believe that individuals have a certain claim in, or interest in, information about themselves. At the same time, I also appreciate the ease and efficiency enabled by a free flow of information, especially in our high-technology, information-driven society. I may choose to share certain information about myself to receive commercial benefits, but I appreciate very much the right to make that choice.

The third core principle is **access**. In many cases, although not all, consumers need access to the information that is collected about them. Information is worthless to a business if it is inaccurate – but for a consumer, the stakes may be much higher. In June, I testified that inaccurate data can have serious consequences for consumers. If consumers have access to their information, they can correct inaccurate information. Of course, we always need to guard against identity thieves seeking to obtain information that is not theirs. But that is not a justification for blocking meaningful access entirely. Consumers should not be forced to endure the spread of falsehoods about who they are, what they owe, and what they do.

The fourth principle of privacy protection is **security**. Consumers should be able to trust that their personal information will be handled securely. Studies show that some consumers are not shopping on the Internet because they fear their personal

information may be stolen. This is a missed opportunity for consumers, businesses, and commerce. For this reason, security worries may have a negative impact on our entire economy.

Of course, certain types of information warrant greater security measures than others. The severity of the harm that is attendant to the potential breach of security surrounding a social security number, for example, is different from the disclosure, I might argue, of your shoe size. When I testified last June, I suggested that we consider whether certain types of information, such as Social Security numbers, should ever be bought, sold or transferred, except for specific permissible purposes, such as law enforcement, anti-fraud measures, and certain legal requirements.[23]

The final core principle of privacy protection is **enforcement**. Without teeth, all of the other principles are meaningless. We have some of the nation's finest law enforcers at the FTC, as well as the strength of the FTC Act behind us. As our track record indicates, our agency is quite capable of enforcing robust privacy laws. But we certainly are not alone. The United States as a whole excels in enforcement. Between the FTC , state attorneys general, myriad federal and state laws, and also private rights of action, privacy invaders have a great deal to fear in this country.

All organizations that handle consumers' data should incorporate these principles into their daily operations. The principles demonstrate a respect for both

the free flow of information and an individual's privacy. The model of notice, choice, access, security, and enforcement facilitates the transmission of better information. It builds a relationship of trust with consumers, employees and businesses.

3. Possession Does Not Necessarily Confer Ownership

While I would not necessarily describe the right to make choices about *"our own"* information as a "property" right, I do believe that individuals should have some type of control and continuing interest in their information, especially if their private individual information is to be used for commercial purposes. In the information age, our information frequently is not in our hands. It is very easy for a company to obtain, compile, and transfer information, simply because it is physically capable of doing so. Former Commissioner Orson Swindle testified that:

> Information security and privacy must become part of the corporate or organizational culture. In today's world, information is currency. Businesses take great steps to protect their money. They need to treat information the same way.[24]

I agree, and I would go even further. A consumer's sensitive, personally identifiable information should be treated much like banks treat a consumer's cash. Banks hold our money in a savings or checking account. They may possess it, but the money is ours, and the bank must provide it when we ask for it. When we are not using that money, however, the bank may use it in certain ways, if we are notified in

advance. We have certain claims to and expectation rights in the money, even though it is not physically in our hands and another entity "possesses" it.

Although a commercial entity may "possess" sensitive personal information, it should realize that it does not necessarily "own" the information, and that the individual may have a competing claim to the control and use of his or her information. If the individual's continuing interest in his or her own information is not adequately recognized, it would be a mistake for both businesses and individuals. Individuals want to trust the businesses they use, and may even want some of their information to be freely shared. If they aren't given notice, however, unauthorized information sharing may lead to consumer anger and resentment. It also may lead to the transmission of inaccurate information – which, in some instances, may cause consumers even greater harm than data breaches.

Thus, even an approach to privacy that focuses solely on avoiding harm and ensuring the free flow of information should recognize that notice, choice, access, security, and enforcement allow for the transmission of better information. Ultimately, I believe that businesses also will benefit from the overarching principle that an individual has an ongoing claim to his or her own data, even when shared in the commercial space. How will businesses benefit? For example, through increased

consumer confidence, both online and in the "bricks and mortar" space; through increased business opportunities; and through intangible business goodwill.

IV. POSSIBLE FUTURE ACTION

Using these principles, what should our plan for future action be? Any future plan should consider what effect our actions will have – on individual consumers, on commerce as a whole, and in the international community.

A. What Businesses Can and Should Do Now

First, even without legislation, all businesses should recognize that, if a commercial entity possesses personal sensitive information, it should treat such information with care, and in a manner worthy of trust. Businesses can and should adopt best practices now – practices that give consumer data the "white glove" treatment. These best practices will build trust with consumers, and building trust builds business. Consumers are affronted when they do not know what companies are doing with their information. Tell them.

Be transparent and judicious about what information you are collecting and why it is being collected. Remember – just because a business *can* collect broad categories of personal data, does not mean that it *should*. It is quite easy to collect information in this technological age, but businesses must step back and ask:

- Why is this information being collected?

– How will it be used?

– Is it necessary for us to collect all of this information?

– What security procedures are necessary to protect such information?

– What security procedures are in place?

– What is the potential harm if such information is misused?

– What is the potential harm if such information is inaccurate?

– What redress would need to be offered to correct such harms?

Many of the companies represented in this room have incorporated the core fairness principles into their business operations. Your companies may be complying with the OECD principles or with the E.U. Directive through the Safe Harbor and Model Codes of Conduct. If so, I applaud your efforts.

As a nation, however, in the area of privacy, I challenge us to do better. A more comprehensive approach to privacy is needed. I am concerned that, internationally, American business will continue to play a diminished role over time, as consumers and governments demand more privacy protection for consumers than our current system is able to offer. Already, parts of Asia, Europe, and Latin America have set the world standard for privacy, and <u>American business is being placed at a competitive disadvantage</u>.

B. Possible Future Legislation

We are very fortunate in this country to have both federal and state enforcement against companies that violate the numerous privacy laws already in place. We also have a vigilant press, which calls companies to task when their poor security practices harm consumers.

But more vigilance is needed. It is my hope that Congress will, at the very least, pass a law providing for: (1) notification to consumers when a data breach creates a risk of identity theft; and (2) civil penalties when a data breach results from poor security practices. As I mentioned earlier, the Commission did not have the authority to obtain civil penalties for BJ's Warehouse or DSW's poor security practices.

In June, the Commission recommended that Congress consider expanding the coverage of the Commission's Safeguards Rule under the Gramm-Leach-Bliley Act. Currently, the Rule only applies to "customer information" created by "financial institutions." It does not cover many other entities that may also collect, maintain, transfer, or sell sensitive consumer information. It should. A broader rule could impose basic safeguarding requirements upon every U.S. business. These steps are an important beginning.

I believe, however, that focusing solely on security breaches and privacy invasions, after they occur, simply does not go far enough. Such an approach focuses only on the harm after it has occurred, but does nothing to foster the development of sustainable best practices for a global economy. Data breach legislation, while perhaps immediately necessary, only continues the "patchwork" approach of legislating reactively, in response to specific events or sectors.

It is time for this country to seriously consider whether overarching privacy legislation is necessary and what such legislation would entail. I understand that Microsoft recently called for comprehensive privacy legislation that would:

– establish a baseline;

– require transparency;

– provide consumers control over personal information; and

– provide for information security, such as safeguards.[25]

Whether we agree or disagree with the specifics of Microsoft's proposal, we all should contribute to the discussion. Our current culture of security should be bolstered by a culture of transparency, in which consumers are told what information about them is collected; how it is used; and how they can make privacy choices. This culture of transparency is necessary not only for the seamless protection of our consumers, but also to ensure the competitive success of American businesses at home and abroad.

I look forward to hearing your thoughts on these issues, and to joining you in this ongoing conversation.

Thank you.

Endnotes

1. These written remarks are a longer version of the speech given before the International Association of Privacy Professionals National Summit.

2. FTC News Release, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *at* http://www.ftc.gov/opa/2006/01/choicepoint.htm.

3. *Id.*

4. *Id.*

5. FTC News Release, *DSW Inc. Settles FTC Charges* (Dec. 1, 2005), at http://www.ftc.gov/opa/2005/12/dsw.htm; FTC News Release, *BJ'S Wholesale Club Settles FTC Charges* (June 16, 2005), at http://www.ftc.gov/opa/2005/06/bjswholesale.htm.

6. *Id.*

7. FTC News Release, *DirecTV to Pay $5.3 Million Penalty For Do Not Call Violations* (Dec. 13, 2005), *at* http://www.ftc.gov/opa/2005/12/directv.htm.

8. *Id.*

9. *See, e.g.,* FTC News Releases, *Book Club Direct Marketer to Pay $680,000 for Do Not Call Violations* (Feb. 23, 2006), *at http://www.ftc.gov/opa/2006/02/bookspan.htm; Columbia House Settles FTC Charges of Do Not Call Violations* (July 15, 2005), at http://www.ftc.gov/opa/2005/07/columbiahouse.htm; *FTC Announces First "Do Not Call" Settlements* (Flagship Resort Development) (Feb. 16, 2005), at http://www.ftc.gov/opa/2005/02/bragliaflagship.htm; FTC REPORT, EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT, A REPORT TO CONGRESS (December 2005), *available at* http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf. (Since the CAN-SPAM Act has been in effect, "the Commission has brought 20 cases alleging violations of the Act.")

10. FTC News Releases, *FTC Shuts Down Spyware Operation* (Enternet Media) (Nov. 10, 2005), *at* http://www.ftc.gov/opa/2005/11/enternet.htm; *FTC Seeks to Halt Illegal Spyware Operation* (Odysseus Marketing) (Oct. 5, 2005), *at* http://www.ftc.gov/opa/2005/10/odysseus.htm; *FTC Cracks Down on Spyware Operation* (Seismic Entertainment Productions) (Oct. 12, 2004), *at* http://www.ftc.gov/opa/2004/10/spyware.htm; *Advertising.com Settles FTC Adware Charges: Free Software Advertised Security Benefits But Didn't Disclose Bundled Adware* (Aug. 3, 2005), *at* http://www.ftc.gov/opa/2005/08/spyblast.htm.

11. FTC News Release, *Two Bogus Anti-Spyware Operators Settle FTC Charges* (Trustsoft and MaxTheater) (Jan. 5, 2006), *at* http://www.ftc.gov/opa/2006/01/maxtrust.htm.

12. FTC STAFF REPORT, SPYWARE WORKSHOP: MONITORING SOFTWARE ON YOUR PERSONAL COMPUTER: SPYWARE, ADWARE, AND OTHER SOFTWARE (March 2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf; FTC STAFF REPORT, RFID: RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS: A WORKSHOP REPORT FROM THE STAFF OF THE FEDERAL TRADE COMMISSION (March 2005), *available at* http://www.ftc.gov/opa/2005/03/rfidrpt.htm.

13. Such laws include the Fair Credit Reporting Act, 15 U.S.C. § 1681; Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401; Cable Communications Policy Act of 1984, 47 U.S.C. § 551; Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2001; Video Privacy Protection Act of 1988, 18 U.S.C. § 2710; Electronic Communications Privacy Act, 18 U.S.C. § 2510; Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201; Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501; Do-Not Call Act, 15 U.S.C. § 6102; Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003), 15 U.S.C. § 7701; and Gramm-Leach Bliley Act (Financial Services Modernization Act of 1999), 12 U.S.C. 1811.

14. Daniel J. Solove, *The Origins and Growth of Information Privacy Law*, 828 PLI/Pat 23 at 52 (May-June 2005). Solove asserts that the FCRA in some respects "involved the lessening of financial privacy" because it "immunizes creditors and credit reporting agencies from lawsuits for 'defamation, invasion of privacy, or negligence' except when the information is 'furnished with malice or willful intent to injure such consumer,'" and also because it has a short, two-year statute of limitations, which, as the U.S. Supreme Court held in *TRW Inc. v. Andrews*, 122 S. Ct. 441 (2001), "begins to run when the violations occurred, not when the individual discovers them."

15. *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

16. *U.S. Senator Ted Stevens (R-AK) Holds a Hearing on Identity Theft Solutions Before the Senate Commerce, Science, and Transportation Comm.* (June 16, 2005) (testimony of Pamela Jones Harbour, Commissioner, Federal Trade Commission), *available at*: CQ Transcriptions, LEXIS ("Harbour testimony"); *see also* http://www.ftc.gov/speeches/harbour/050616idthefttest.pdf.

17. U.S. DEP'T OF HEALTH, EDUCATION, AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (July 1973) (Summary and Recommendations).

18. ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER

FLOWS OF PERSONAL DATA, (1980) *at* http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html. ("Basic Principles of National Application"). The OECD guidelines refer to the following eight principles: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness principle; individual participation; and accountability. ASIA-PACIFIC ECONOMIC COOPERATION, APEC PRIVACY FRAMEWORK, (2004) *available at* http://www.apec.org/apec/enewsletter/march_vol2/onlinenewse.html. The APEC Privacy Framework refers to the following nine principles: preventing harm; integrity of personal information; notice; security safeguards; collection limitations; access and correction; uses of personal information; accountability; and choice.

19. FTC REPORT, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998) at 7, *at* http://www.ftc.gov/reports/privacy3/priv-23.htm [*hereinafter* 1998 PRIVACY ONLINE REPORT].

20. *See, e.g.*, Sheila Anthony, [Former] Commissioner, Federal Trade Commission, Remarks before The First National HIPPA Summit (Oct. 15-17, 2000), *at* http://www.ftc.gov/speeches/anthony/hippa.htm; Testimony of Sheila Anthony, [Former] Commissioner, Federal Trade Commission, on Online Privacy Protection, Before the U.S. Senate Committee on Commerce, Science, and Transportation (May 25, 2000), *at* http://www.ftc.gov/speeches/anthony/tstmyprivacy000525.htm; Statement of Robert Pitofsky, [Former] Chairman, Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 22, 2000), *at* http://www.ftc.gov/reports/privacy2000/pitofskystmtonlineprivacy.htm.

21. *Self-Regulation and Privacy Online Before the Subcomm. on Communications of the Senate Comm. on Commerce, Science, and Transportation*, (July 27, 1999), (prepared statement of the Federal Trade Commission at 14, n.22), *available at* http://www.ftc.gov/os/1999/07/privacyonlinetestimony.pdf; *see also* 1998 PRIVACY ONLINE REPORT, *supra* note 19, at 7.

22. Harbour testimony, *supra* note 16. The prepared testimony of the Commission, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION BEFORE THE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, U.S. SENATE, ON DATA BREACHES AND IDENTITY THEFT (June 16, 2005), at http://www.ftc.gov/os/2005/06/050616databreaches.pdf, at 7 and n. 16, states: "The Commission recommends that Congress consider requiring companies to notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft. Commissioner Harbour is concerned about the use of the term 'significant' to characterize the level of risk of identity theft that should trigger a notice to consumers." In 2004, the Commission's prepared testimony stated: "*If information that creates a risk of identity theft has been stolen, however, the FTC suggests notifying individuals of the incident as soon as possible so they can take steps to limit the potential damage*." Prepared Statement of the Federal Trade Commission before

the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census Committee on Government Reform, U.S. House of Representatives, *Protecting Information Security and Preventing Identity Theft*, Sept. 22, 2004 (emphasis added), at 5, *at* http://www.ftc.gov/os/2004/09/040922infosecidthefttest.pdf.

23. Harbour testimony, *supra* note 16.

24. *U.S. Senator Ted Stevens (R-AK) Holds a Hearing on Identity Theft Solutions Before the Senate Commerce, Science, and Transportation Comm.* (June 16, 2005) (testimony of Orson Swindle, former Commissioner, Federal Trade Commission) *available at*: CQ Transcriptions, LEXIS.

25. Brad Smith, Senior Vice President, General Counsel and Corporate Secretary, Microsoft Corp., *Protecting Consumers and the Marketplace: the Need for Federal Privacy Legislation* (Nov. 2005), *available at* http://www.microsoft.com.