"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.

---

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

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 a

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 diffe

differing notions of what privacy *should* be? How can we reach a common understanding – one that can form the basi

---

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

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]

Th13.77in5 T1d,ecoprinci, i3.98(tiBT/TT0 1r. Span 5gh74ume3MTw 132 e,7s 0 0 13.98

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

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

- 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

B. Possible Future Legislation

We are very fortunate in this country to have both federal and state enforcement

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

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 SM5osARE WORKSHOP: MONITORING S

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 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.