



de·fin·ing

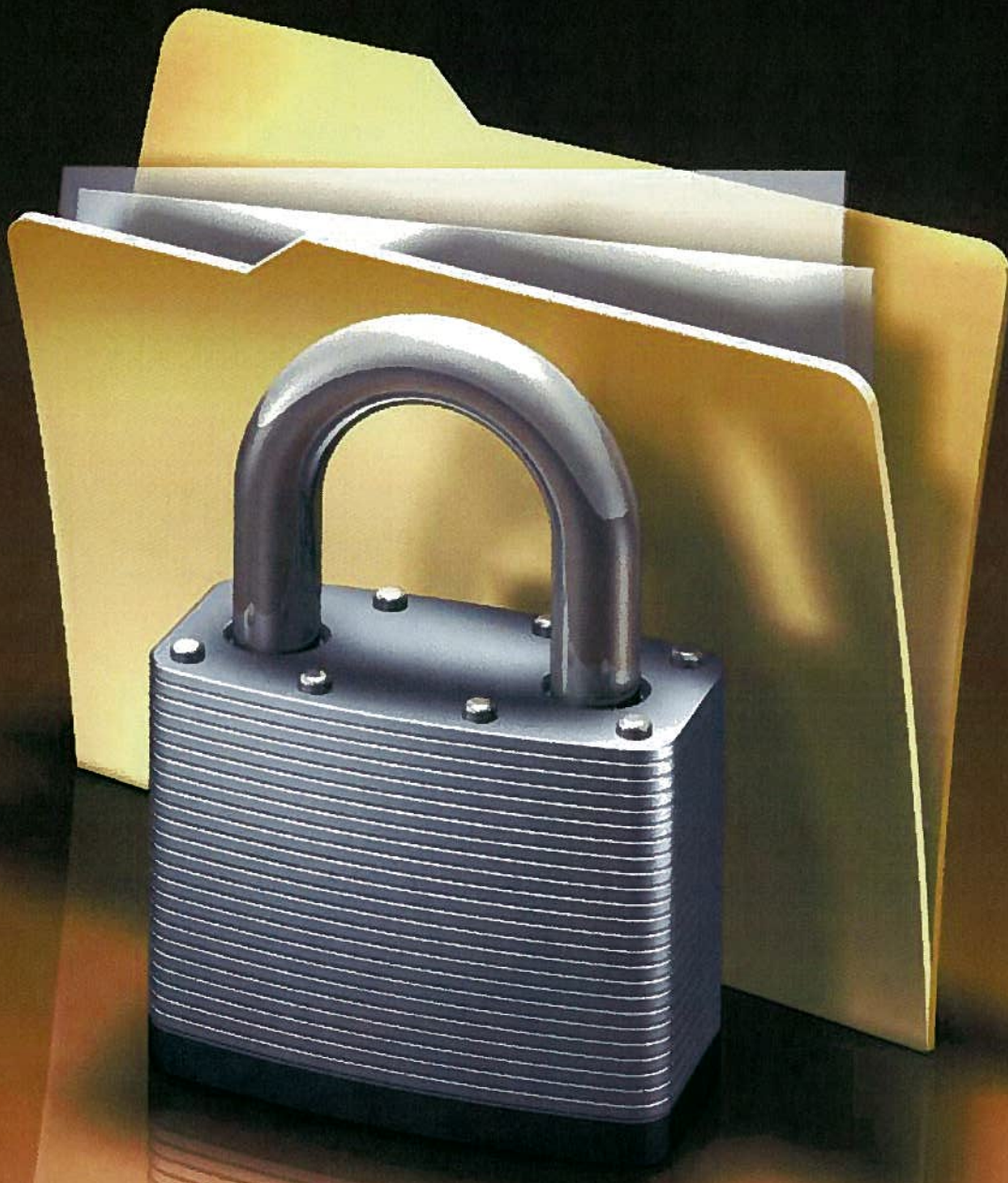
By Michael C. Lamb and Ronald I. Raether, Jr.

For years, outside of certain regulated industries and a few cutting-edge businesses, the focus was on perimeter security, with less attention to application data security and compliance issues. On February 15, 2005, there was a dramatic and fundamental shift in management's focus on security: ChoicePoint announced that it was a victim of a security breach and that unauthorized persons were able to gain access to consumer information. Since that date, until May 2006, there have been over approximately 3800 additional announcements of security data breaches potentially affecting the personally identifiable information of as many as 167 million people.¹

Data security and compliance issues are now at the forefront as a concern for both citizens and the management of businesses. While legal standards for information security for many businesses remain uncertain, one point has become clear in the last year: No business is immune from having to address the issue of data compliance and security. For companies operating in regulated industries, experience may exist to develop and implement appropriate measures to protect sensitive personal information. Other companies, however, may be starting from scratch. Regardless of prior experience, a universal question persists—what standard needs to be met?

Data Security Measures

That Protect Your Company and Customers



What the FTC Says and Doesn't Say

The phrase adopted by the Federal Trade Commission (FTC), and often repeated, is that every business "[should] maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information."² Implementing measures to satisfy this general (and vague) standard is difficult. Moreover, rapidly developing technology, variations in business requirements, the type and form of personal data received, the applicability of varying laws and state and federal enforcement authority, and countless other issues, make it unlikely that a universal legal standard that provides clear rules will ever be developed.

Instead, the nature of each company's business, including an inventory of what information is collected and where it is retained, will dictate the measures that must be implemented to ensure the protection of sensitive information. Different types of information require different measures of security. For example, a business that routinely handles credit card numbers requires a higher level of protection than a business that holds little more than a street address.

"[While] there is no such thing as perfect security, breaches can happen even when a company has taken every reasonable precaution," said Deborah Platt Majoras, Chairman of the Federal Trade Commission before the 2005 Congress at the hearing, "Data Breaches and Identity Theft: Hearing Before the Senate Comm. on Commerce, Science, and Transportation." Businesses can look to a number of different sources for guidance to develop standards to protect sensitive information. This article will discuss three of those sources:

- the Gramm-Leach-Bliley Act or Financial Services Modernization Act of 1999 (GLBA);
- enforcement actions by the FTC; and
- commonalities in standards adopted by the government and various organizations including the Payment Card Industry (PCI) Data Security Standard; ISO/IEC 17799 and ISO/IEC 27001; SAS70, and WebTrust and SysTrust (developed by the American Institute of Certified Public Accountants); and EU Directive 95/46/EC, European Union Data Protection Directive.

How the GLBA Affects Your Data Protection Policies

The GLBA is illustrative for many reasons, including continuing reference to the GLBA as a guide for developing standards for the various notification bills pending be-



MICHAEL C. LAMB is vice president and general counsel for LexisNexis Risk and Information Analytics Group in Boca Raton, FL. His corporate practice includes a particular emphasis on information privacy, security, and technology matters. He is a former chief privacy officer for AT&T and has testified before Congress on privacy matters. He can be reached at michael.lamb@lexisnexis.com.



RONALD J. RAETHER, JR. is a partner with Faruki Ireland & Cox PLL, where he practices in the area of technology-related litigation and privacy compliance—matters ranging from compliance audits and reviews to class actions regarding software applications and federal privacy statutes. He has lectured on a variety of litigation and compliance issues, including managing electronic discovery and complying with data privacy regulations. He can be reached at raether@ficlaw.com.

fore Congress. The GLBA regulates the collection, use, and disclosure of consumer financial information by "financial institutions" (e.g., non-bank mortgage lenders, loan brokers, and some financial or investment advisers). 15 U.S.C. § 6801. The major components regarding privacy protections in the GLBA include the Financial Privacy Rule and the Safeguard Rule, which were promulgated by the Federal Trade Commission (FTC).

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice upon the establishment of the consumer relationship and then provide further notice in each subsequent year.³ Generally, the privacy notice must explain the information collected about the consumer, where that information is stored, how that information is used, and how that information is protected. The notice also must identify the consumer's right to opt-out of the information being shared with unaffiliated parties.

The Safeguard Rule requires financial institutions to develop a comprehensive written information security plan that contains reasonable administrative, technical, and physical safeguards, and measures for continuing to evaluate the plan and force adjustments to the plan based on the evaluation.⁴

Generally, the plan must include:

- designation of one or more employees to coordinate the information security program;
- identification of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessments of the sufficiency of any safeguards in place to control those risks;
- implementation of information safeguards to control the risks identified through risk assessment, and regular tests of the effectiveness of the safeguards' key controls, systems, and procedures;
- overseeing service providers; requiring them to protect the security and confidentiality of customer information; and
- evaluation and adjustments to the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

An evaluation of the record of FTC enforcement actions provides further guidance on standards to pursue in developing a compliance and security program, providing further definition to the Safeguard Rules. Although not written as

a privacy law, the FTC has been using the Federal Trade Commission Act (FTCA), 15 U.S.C. §§ 41-51, to regulate and protect personal information. Section 5 of the FTCA provides the Federal Trade Commission with enforcement authority over “unfair or deceptive acts or practices.”⁵

The FTC enforces the substantive requirements of Section 5 through both administrative and judicial processes. In the administrative process, the FTC makes the initial determination whether the practice is an unfair or deceptive trade practice. When the FTC determines that there is reason to believe that an unfair or deceptive trade practice has occurred, it may issue a civil investigative demand and ultimately a complaint setting forth its charges. Faced with a possible complaint, a party may elect to accept and submit to a consent agreement without admitting liability.

Many of the first privacy-related enforcement actions filed by the FTC focused on the “deceptive” leg of the FTCA. These cases point to one of the first places to start a comprehensive review of security practices, specifically

These cases point to one of the first places to start a comprehensive review of security practices, specifically a company’s public statements on privacy and security.

a company’s public statements on privacy and security. Beginning in early 2000, it became common practice for businesses to develop and sponsor “Privacy Statements.” In these statements, companies would provide assurances to consumers about how their information would be handled, to whom it would be distributed, and in some instances the level and form of security applied to the information.

In early 2002, the FTC relied on the “deceptive” leg of the FTCA in reaching a settlement with Eli Lilly & Company (Lilly), which had inadvertently disclosed the email addresses of the subscribers to its Prozac® mailing list.⁶ Lilly inadvertently sent a form email to subscribers of the mailing list concerning its Prozac® medication that disclosed all of the subscribers’ email addresses to each individual subscriber by including all of their addresses within the “To:” entry to the message. The disclosure was contrary to the company’s privacy statement as Lilly promised that all information submitted by customers, including email addresses, would be kept confidential and that the company had security measures in place to maintain the

privacy of information. The FTC argued that Lilly had not instituted appropriate security measures as Lilly:

- “failed to provide appropriate training for its employees” regarding security,
- “failed to provide appropriate oversight and assistance to employees to ensure compliance with written security requirements,” and
- “failed to include security in the testing process to avoid inadvertent disclosure of sensitive information.”

In other words, despite the representations in its Privacy Statement, Lilly did not have oversight controls in place to achieve its publicly stated security goals.

Lilly was not alone in being held accountable for their public statements on privacy and security after a data breach. Microsoft, Guess?, Inc., Petco, Tower Records, and others have faced similar actions. Other guiding principles distilled from these enforcement actions include:

- designing systems to avoid unauthorized access with reasonable identification and authentication procedures (i.e., unique IDs and passwords);
- implementing tools to detect unauthorized access that include the retention of system information to conduct such reviews;
- protecting against commonly known or reasonably foreseeable attacks from unauthorized users (e.g., SQL injection attacks in Guess?, Inc., Petco, and November 2006, Guidance Software, Inc.); and
- encrypting sensitive personal information and user passwords not only in transit, but also in storage (where the Privacy Statement promised that the data would be handled by SSL encryption).

The policies addressing security obviously need to be consistent with Privacy Statements made to and for the benefit of the public.

The FTC findings in these matters are instructive even in the absence of Privacy Statements, as many of the Privacy Statements made general representations about security, such as employing “reasonable” measures. In sum, these cases illustrate the importance of being proactive in responding to potential threats and, as recently stated by the FTC, “implement[ing] simple, inexpensive and readily available security measures to protect consumers’ data.”⁷ Anyone involved in data security knows that these threats are always evolving. For example, two years ago the threat came from “hobby” hackers tempted by the “game” of trying to beat perimeter security. Today, while these threats still exist, criminals are using hacking techniques that get behind perimeters with valid user credentials and then seek to exploit vulnerabilities in the application code.⁸ The above cases illustrate the need to have system controls in place to track unusual usage patterns, and to provide system data to permit forensic studies to pursue potential unauthorized access.⁹

In June 2005, the FTC announced a settlement with BJ's Wholesale Club, Inc. (BJ's).¹⁰ Unlike the cases involving alleged deceptive practices, BJ's did not have a written privacy policy that made assurances of a certain level of data protection. Instead, the FTC looked at BJ's security procedures and deemed them to be insufficient, charging BJ's with engaging in conduct unfair to consumers. By this enforcement action, the FTC signaled to companies that the "unfairness" leg of the FTCA created some undefined reasonableness standard with regard to the protection of consumer data. In other words, it is no longer sufficient merely to seek and satisfy any security assurances made in a Privacy Statement. Companies must also continually evaluate their operations and the consumer data they handle to develop and implement a program that maintains and enforces internal measures appropriate under the circumstances to protect sensitive information.

With the BJ's action, the FTC provided further guidance as to what conduct was deemed to be unreasonable and inappropriate. Specifically, the FTC found that BJ's:

- did not encrypt credit card numbers while in transit or when stored on the in-store computer networks;
- stored the information in files that could be accessed anonymously—i.e., using a commonly known default user id and password;
- did not use readily available security measures to limit access to its computer networks through wireless access points on the network;
- failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and
- created unnecessary risks to the information by storing it for periods in excess of the limits established by certain banking rules and regulations.

In December 2005, the FTC announced another settlement relying on the "unfairness" leg of the FTCA, this time with DSW, Inc. (DSW).¹¹ The settlement stemmed from DSW's March 2005 announcement that a security breach resulted in the potential release of over 100,000 individuals' personal information. The FTC found that DSW created unnecessary

ACC Extras on... Data Security

ACC Docket

- *Nine Contractual Items to Consider Before You Outsource Your Company's Data Center* (January/February 2007). As companies grow increasingly reliant on their IT systems, they have turned to third party providers to alleviate some infrastructure concerns. Learn more about how to choose an outside contractor so that your company's information is safeguarded while still meeting your budget forecasts. www.acc.com/resource/v8046
- *Trends in Discovery of Electronically Stored Information* (January/February 2007). What more could you ask for than a judge's perspective from the bench? What do lawyers overlook during ediscovery? Find out about ediscovery trends that will help you when the time arrives. www.acc.com/resource/v8044

InfoPAKsSM

- *Email and the Internet* (2007). Employee access to the internet and email, employer regulation and monitoring of internet use, and new issues presented by the increased use of electronic means of communication and their effect on the process of discovery are all addressed in this InfoPAK. www.acc.com/resource/v6263
- *Data Protection—A Practical Guide* (2006). This InfoPAK provides a general overview of the key issues that all US businesses should be aware of if they are requesting information about individuals to be transferred from Europe or Canada into the United States. www.acc.com/resource/v6283

Program Materials

- *Leading the Way in Privacy and Data Security Compliance* (Annual Meeting 2006). A growing area of regulatory and legislative activity is data security. Aside from legal implications, data breaches can wreak havoc on a business, damaging customer or employee confidence. Learn where the law in this area is headed, and take home a step-by-step guide to best practices in preparing for and responding to data breaches. www.acc.com/resource/v8197

Quick References

- *Complying with Data Security Breach Laws* (2006). These guidelines will help companies to quickly and efficiently comply with the varying state data privacy laws. www.acc.com/resource/v7501

Webcasts

- *Protecting Individual Information: A Guide for In-house Counsel* (2007). If your company maintains personal or sensitive information and has a data breach, are you prepared? The panel on this webcast covered key principles to guide your company's privacy and information security plan. www.acc.com/resource/v8607

ACC has more material on this subject in our Virtual LibrarySM. To create your personalized search, visit www.acc.com, click on the "Research" pull down menu button, then select Virtual Library. Type in your keywords and search to see the other resources we have available.

risks to stored personal information by failing to employ sufficient measures to detect unauthorized access. In addition, the FTC found that DSW retained personal information in multiple files and stored the information in an unencrypted format, which could be easily accessed by using a commonly known user ID and password. The commission also found that DSW did not use readily available security measures to limit access to its computer network through wireless access points on the network, and that it did not sufficiently limit the ability of computers on one in-store network to connect to computers in other in-store and corporate networks.

Continuing to pursue companies that failed to exercise generally accepted standards, the FTC launched an investigation into ChoicePoint's privacy, verification, and compliance practices. The FTC found that ChoicePoint failed to verify properly the identities of customers before providing those customers with access to consumers' personal information.¹² More specifically, ChoicePoint had accepted "facially contradictory or illogical application information [] without conducting further inquiry to resolve apparent anomalies." Further, the FTC found that ChoicePoint failed to monitor or otherwise identify unauthorized activity, even after it was notified by law enforcement of fraudulent activity between 2001 and 2004, and despite its knowledge of suspicious activity. For example, ChoicePoint continued to provide a high volume of reports even after the subscriber's telephone had been disconnected, the address was incorrect, and the credit card was not associated with the subscriber. Additionally, the FTC stated that ChoicePoint made false and misleading representations to both customers and the public about the safeguards employed to protect the security of information and ensure compliance with the FCRA.

Looking at the glass from the other side, on June 5, 2007, the FTC issued a closing letter in an investigation into possible Section 5 violations relating to the breach involving Dollar Tree Stores, Inc. (Dollar Tree).¹³ Dollar Tree had been the victim of a "PED skimming" scheme, where a malicious memory chip was secretly placed in the PIN entry device (PED) used at the point of sale to process payment card purchases. The hidden memory chip was later collected by the criminals, from which the criminals could extract the consumer's personal information, including the magnetic stripe data and the PIN associated with a particular card.

The FTC decided not to pursue an action after apparently deciding the "risk at issue was [not] reasonably foreseeable at the time of the compromise." Providing a road map as to what might persuade the FTC of Section 5 compliance, other important factors were: "[1] the nature and magnitude of the risk relative to other risks; [2] the benefits relative to the costs of protecting against the risk; [3] Dollar Tree's overall data security practices; [4] the duration and scope of the compromise; [5] the level of consumer injury; and [6] Dollar

Tree's prompt response." For Dollar Tree, prominent among these factors was the short time frame in which PED skimming was known by security experts as a risk. The FTC distinguished DSW and other recent enforcement actions based on the failure in those cases by the company to use inexpensive and available solutions to address "well-known" vulnerabilities that resulted in "substantial injury to consumers in the form of account fraud, time loss, and inconvenience."

While not a silver bullet, the private and government standards can help in-house counsel to guide the development of standards appropriate to company's business.

In-house Counsel's Five Step Roadmap

The FTC enforcement actions and now closing letter, along with the GLBA Safeguard Rules, provide a five-step roadmap to developing a security plan: (1) assess the risks; (2) develop a plan; (3) follow the plan; (4) periodically reevaluate the plan; and (5) alter the plan based on the reevaluation. Some of the common areas in-house counsel can evaluate potential risk include: (a) program oversight (i.e., accountability); (b) user identification and authentication procedures; (c) security controls in research and development; (d) third-party vendors and service providers; (e) data use rules (is it necessary and how is the data stored and transmitted); (f) employee and user education; (g) data usage monitoring; (h) tools to permit detection of unauthorized use; and (i) retention of data to permit forensic studies of suspected unauthorized use.

Numerous standard setting organizations have worked to define a process to help companies improve compliance with a general reasonableness standard. In-house counsel can see that their company:

- designates one or more employee(s) to coordinate the safeguards;
- identifies and assesses the risks to consumer information in each relevant area of the company's operation;
- designs and implements a safeguards program, and regularly monitor and test it;
- selects appropriate service providers and contract with them to implement safeguards;
- evaluates and adjusts the program in light of relevant circumstances, including changes in the firm's business operations, or the results of testing and monitoring of safeguards; and

- disposes of customer information in a secure manner by hiring or designating a records retention manager to supervise such disposal; shreds or recycles customer information; erases all data when disposing of computers, diskettes, magnetic tapes, hard drives, etc.; effectively destroy the hardware; and promptly dispose of outdated customer information.

In-house counsel should work with the IT team so that they identify and analyze gaps in the current security procedures and then design and implement solutions to close those gaps and ensure ongoing conformity. Tests should be conducted to discover vulnerabilities and security flaws in computer networks and track emerging internet threats. Companies should conduct penetration tests (ethical hacking) that simulate covert and hostile network attack activities to identify specific exploitable vulnerabilities and to expose potential electronic entryways to sensitive data. Companies also should consider conducting an application review that identifies security flaws behind the firewall, such as SQL Injection, cross-site scripting, buffer overflows, and the like. For more information on these technical terms, see the Web Security Glossary from the Web Application Security Consortium, available at www.webappsec.org/projects/glossary. Whether the company conducts these tests with internal resources or hires an external third party will depend upon the resources available to the company. Under either circumstance, these tests should be conducted under the supervision of the general counsel's office and/or outside counsel to improve privilege arguments.


No Silver Bullet Will Protect Your Company

Security standards established by government agencies provide another useful resource to identify measures that improve the likelihood of establishing the reasonableness of an information security plan. A recent example arose after the Department of Veterans Affairs announced the theft of a laptop computer on which unencrypted personal information was stored. Information on Veterans Affairs Data Security Issue, is available at www1.va.gov/opa/data/data.asp. In a memorandum from Clay Johnson III, Deputy Director for Management, the Office of Management and Budget on June 23, 2006,¹⁴ the White House announced standards for the protection of sensitive agency information on laptop computers and other remote devices. Among other points, the memorandum referenced a checklist developed by the National Institute of Standards and Technology and required:

- data to be encrypted unless designated in writing to be non-sensitive;
- two-factor authentication;
- require the "time-out" function to lock the computer after 30 minutes of inactivity; and

- logging of all data that is stored on the remote device and requiring its removal after 90 days unless use is still required.

While not a silver bullet, the private and government standards can help in-house counsel to guide the development of standards appropriate to company's business. The above discussion provides a starting point for developing an information security program that maintains and implements internal measures appropriate under the circumstances to protect sensitive information.

In the end, expertise both as to the company's practices and as to general industry norms will be important in crafting a security plan that protects the company against claims of negligently handling protected data. At the moment, the standard for reasonable data security is not unlike the standard described by United States Supreme Court Justice Potter Stewart for identifying pornography—"I know it when I see it."¹⁵ With the help of a knowledgeable team of business people, security and technical personnel, and lawyers, companies can develop defensible and effective data security plans. 

Have a comment on this article? Email editorinchief@acc.com.

NOTES

1. Privacy Rights Clearinghouse, "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," at www.privacyrights.org/ar/ChronDataBreaches.htm, last visited on October 5, 2007.
2. *Eli Lilly & Company; Analysis to Aid Comments, Proposed Consent Agreement*, 67 Fed. Reg. 4963, 4964 (February 1, 2002).
3. Privacy of Consumer Financial Information, 16 C.F.R. § 313 (2000).
4. Standards for Safeguarding Customer Information 16 C.F.R. § 314 (2002).
5. 15 U.S.C. § 45(a)(1).
6. *Eli Lilly & Company; "Analysis to Aid Comments, Proposed Consent Agreement."* 67 Fed. Reg. 4963, 4964 (February 1, 2002).
7. "Guidance Software Inc. Settles FTC Charges," at www.ftc.gov/opa/2006/11/guidance.htm.
8. Paul F. Roberts, "SANS Warns of Attack Shift to Apps, Network Devices," *Eweek.com*, November 22, 2005, available at www.eweek.com/article2/0,1895,1892115,00.asp.
9. Ellen Messmer, "Niksun's Tools Track Network Traffic (and Hackers?) for Comdex," *PC World*, November 13, 2000, available at www.pcworld.com/resource/article/0,aid,34705,00.asp.
10. *BJ's Wholesale Club, Analysis of Proposed Consent Order to Aid Public Comment*, 70 Fed. Reg. 36939 (June 27, 2005).
11. *DSW, Inc., Analysis of Proposed Consent Order to Aid Public Comment*, 70 Fed. Reg. 73474 (December 12, 2005).
12. *United States of America v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga. filed Jan. 30, 2006).
13. www.ftc.gov/os/closings/staff/070605doltree.pdf.
14. Available at <http://whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf>.
15. *Jacobellis v. Ohio*.