Privacy Officers ADVISOR

iapo international association of privacy officers

The official monthly newsletter of the International Association of Privacy Officers

July 2002 | Editor: Marilou M. King, Esq. | Volume 2, Number 10

FTC Standards for Safeguarding Customer Information

Patrick F. Sullivan, PhD

On May 17, 2002, the Federal Trade Commission released its final rule for 501(b) security safeguards required under the Gramm-Leach-Bliley Act (GLBA). The FTC safeguards rule reflects the security guidelines issued by the banking agencies and NCUA but has incorporated language to make the requirements as flexible as possible to apply to the wide range of institutions regulated by the FTC and to reduce the burden on "smaller and less sophisticated" institutions of implementing the safeguards. This creates some specific contrasts with the banking agency guidelines that have potential implications for the security programs of institutions covered by the FTC safeguards rule.

Because of the types of entities covered by the rule, including service providers that may be covered by other safeguards regulation, and financial institutions that receive customer data from other institutions but themselves do not have any customer data, several distinct issues pertaining to the scope of the FTC safeguards rule were raised in the comments. These issues are:

- whether the FTC safeguards rule should apply to financial institutions that receive customer information but do not collect their own customer information;
- whether institutions should be responsible for the safeguards of their affiliates and service providers;
- whether compliance with alternative standards can be deemed as compliance with the FTC safeguards rule; and
- whether certain entities can be excluded from the definition of "service provider."

Following is an overview of the FTC safeguards rule and comparison on key points with the banking agency guidelines, together with discussion of how the above issues were addressed by the FTC.

Basic Scope and Requirements

Entities covered by the FTC safeguards rule are required to "develop, implement and maintain a comprehensive information security program" with administrative, technical

*See **Standards**, page 2*

New European Union Directive

Bans Spam, Limits Cookies

Ray Everett-Church

On May 30, 2002, the European Parliament approved a set of sweeping new guidelines that affect an array of online and offline marketing practices, including limitations on the usage of Web browser "cookies" and restrictions on various electronic communications, including a ban on e-mail "spam."

The memorably titled "European Parliament legislative resolution on the Council common position for adopting a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector" addresses many online marketing practices, from cookies and spam to

*See **Directive**, page 5*

This month:

Privacy Officers Advisor

Editor
Marilou M. King, Esq.
McDermott, Will & Emery
Phone: 202/756-8244
E-mail: mking@mwe.com

Section Editors
Health:
Cindy Nichols, HCA Healthcare
cindy.nichols@hcahealthcare.com

Government Contracts:
Craig Holman, Holland & Knight
caholman@hklaw.com

Internet:
Ray Everett-Church, ePrivacy Group
ray@eprivacygroup.com

Financial Services:
Patrick Sullivan, Guardent
patrick.sullivan@guardent.com

Telecommunications:
Douglas McCollum, CoreFacts
dmccollum@corefacts.net

To subscribe, call:
800/266-6501

For customer service, call:
800/266-6501

Advertising and sales
Phone: 800/266-6501

Managing Editor
Nancy Gray Puckett
Phone: 312/938-2116
E-mail: npuckett@mindspring.com

Production Editor
Douglas M. Burnette

Privacy Officers Advisor (ISSN: **1532-1509**) is published monthly for $199 per year by the International Association of Privacy Officers
1211 Locust Street
Philadelphia, PA 19107

Phone: 800/266-6501

Postmaster:
Send address changes to:
IAPO
1211 Locust Street
Philadelphia, PA 19107

Subscription price: $199 per year, plus postage, handling, and appropriate state sales tax.

Business and circulation:
IAPO
1211 Locust Street
Philadelphia, PA 19107

Requests to reprint:
Nancy Gray Puckett
Phone: 312/938-2116
Fax: 312/938-8683
E-mail: npuckett@mindspring.com

Standards

from page 1

and physical safeguards that are appropriately designed to address the size and scope of the entity's operations and the sensitivity of data handled. In its response to comments, the FTC stressed the flexibility implied by the language defining the information security program requirement.

Both the banking agency guidelines and FTC safeguards rule apply to the protection of customer information. The FTC cautions, however, that institutions may apply safeguards to consumer information as well, where customer and consumer information cannot reliably be separated. In addition, the FTC in its discussion recognizes that some security controls may support consumer preference (opt-out) management, and where organizations elect to merge consumer and customer data for certain marketing purposes, those security controls supporting preferences would also potentially cover consumer information.

Because the safeguards apply to customer information, and because the FTC believes that the provisions applying to service providers and affiliates do not adequately address all third-party data sharing relationships, the commission determined that the safeguard rule will apply to institutions that receive but do not collect their own customer information. In addition, institutions are responsible for ensuring the safeguards of their affiliates and service providers, in the latter case, as discussed below, through contracts discussed below.

Customer information is defined as "any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates." Because the definition extends the meaning of customer information to data handled by affiliates, the requirement to ensure the safeguards of customer information also extends to ensuring the affiliate's safeguards. Such institutions have obligations with respect to their own safeguards of customer information and duties with respect to ensuring the safeguards of their affiliates. This means that institutions with responsibility for affiliate's safeguards will need well-coordinated implementation and management of security programs across the enterprise.

As with the financial institutions subject to the banking agency guidelines, institutions subject to the FTC safeguards rule must have a written program that, the FTC clarifies, can exist as a series of coordinated documentations across program elements and business functions rather than a single written document. It is important, then, in building a program to meet the FTC safeguards rule that an organization carefully and thoroughly identify and inventory the written policies and procedures that define the required elements and processes of its security program. The absence of written policies should, of course, be noted as a gap in the organization's initial risk assessment to establish its baseline needs and specific objectives for its information security program. Managers and employees responsible for maintaining information security should have ready access to the written policies that define the security program, regardless of how the policies are stored across the organization.

Accountability Structures

While the banking agency guidelines require board approval and oversight of an institution's security program, including implementation and maintenance, they do not require institutions to focus accountability for implementation in an individual by creating a corporate (of chief) information security officer (CISO) position.[1] In addition, rather than concentrating accountability for day-to-day management of the program in an individual or functional level of an institution, specific management responsibilities to review and adjust the program, document compliance, and report on the status of the program to the board are distributed across provisions of the guidelines.

By contrast, to balance the implementation and oversight responsibilities assigned to boards with the need to address the organizational contin-

gencies of smaller entities regulated by the FTC, the FTC safeguards rule requires entities to "Designate an employee or employees to coordinate [the organization's] information security program." This can mean that the role or functions of a CISO need to be defined for an organization. At a minimum, this requirement means that, especially for larger organizations, information security management roles, responsibilities, and accountabilities must be well defined, identified and, coordinated across the relevant business functions or identified risk areas.

Risk Assessment and Program Design

Consistent with the banking agency guidelines, the FTC safeguards rule requires institutions to:

> Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

Part of the risk assessment under the banking agency guidelines includes assessing the "likelihood and potential damage" of threats, as well as the "sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risk."

The FTC safeguards rule specifies the following as minimum necessary considerations in risk assessment:

- employee training and management;
- information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
- detecting, preventing, and responding to attacks, intrusions, or other systems failures.

Intrusion detection and penetration testing, for example, should be viewed as critical areas of initial risk assessment as well as key testing and monitoring activities to ensure maintenance of the security program at appropriate levels of control and to help ensure ongoing compliance of the institution with its policies and the FTC safeguards rule. By adding "network and software design" to the considerations, the FTC safeguards rule underscores the integral relationship of security controls to ensuring privacy and reducing the risk of a privacy failure or enforcement action as a result of a security breach or failure. Security controls in network and software design are also integral to upholding key fair information practices such as consumer choice or access or regulatory restrictions on data flow such as restrictions on disclosure of account identifying information. Thus risk assessment may need to consider the appropriateness and practicality of specific security technologies such as biometrics, as well as the security controls around information management software.

In light of the consent agreement with Eli Lilly (see the March 2002 issue of this newsletter), in which a failure of the security program tied to employee supervision and training resulted in a privacy enforcement action, it is no surprise that employee training and management would be a minimum required consideration for risk assessment. Staff training to implement the security program is also specifically called out as an element of risk management and control in the banking agency guidelines.

The FTC safeguards rule offers little general guidance on steps or processes to manage and control risk once the risk assessment is complete. Rather, the FTC safeguards rule requires institutions to:

> Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

The banking agency guidelines outline eight specific types of security measures and require banks to consider whether each is appropriate for the institution and adopt those that are, thereby providing some direction on steps or processes to implement. These include access controls and restrictions, encryption of customer information, procedures to review

*See **Standards**, page 4*

iapo international association of privacy officers

International Association of Privacy Officers

1211 Locust Street
Philadelphia, PA 19107

Phone: 800/266-6501 or 215/545-8990

Fax: 215/545-8107

E-mail: information@privacyassociation.org

Privacy Officers Advisor is the official monthly newsletter of the International Association of Privacy Officers. All active association members automatically receive a subscription to *Privacy Officers Advisor* as a membership benefit. For details about joining IAPO, please use the above contact information.

Standards

from page 3

impacts on the security program of new information management technologies, dual control procedures, intrusion detection and penetration testing, and incident response and disaster recovery processes. In response to comments and the need to provide only a general direction in its rule in order to maintain the flexibility of the rule for smaller organizations, the FTC has promised to issue educational materials to assist organizations with compliance.

Oversight of Service Providers

As with the banking agency guidelines, the FTC safeguards rule requires oversight of service providers. The banking agency guidelines require a due-diligence process based on risk assessment of the service provider relationship and require institutions to impose contractual requirements that the service provider maintain controls that meet the objectives of the guidelines. The FTC safeguards rule requires that institutions take "reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue" and contractually require service providers to implement and maintain those safeguards.

The commission recognizes that some service providers will be financial institutions themselves or will also be service providers to institutions covered under the banking agency guidelines. However, the allowance for the use of alternative safeguards as a means for complying with the FTC safeguards rule is limited. Institutions that can demonstrate their compliance with the banking agency guidelines will meet the FTC safeguards rule. While compliance with other safeguards requirements will be considered in determining compliance with the FTC safeguards rule, the commission is clear that other safeguards do not always provide the same or similar scope or requirements of protection. While the FTC is counting on the flexibility of its guidelines to lessen the burden on institutions that are subject to multiple security regulations, such institutions will need to thoroughly assess and inventory all of their security controls and consolidate their documentation in a way that enables easy identification of elements that meet the FTC safeguards rule. In other words, the organization of policies and practices to meet multiple compliance obligations should be undertaken from the perspective of enterprise security and privacy management; compliance risk increases where responsibility for risk assessment, program implementation, and program management are overdistributed.

The commission also flatly refused to exclude certain professional organizations and other institutions from the scope of organizations that meet the definition of "service provider" under the rule. The FTC believes that this parallels the banking agency guidelines, which also offer no exceptions, and that even where the institution is subject to professional rules that address confidentiality of customer or client data (*e.g.,* law firms or accounting firms), these professional rules do not cover all of the areas of security protection addressed in the FTC safeguards rule. For example, such professional rules do not address service provider agreements or affiliate controls.

Program Monitoring and Adjustment

As with the banking agency guidelines, the FTC safeguards rule requires institutions to monitor and adjust their security programs. Specifically, institutions must:

> Evaluate and adjust [their] information security program in light of the results of the testing and monitoring required [under program design]; any material changes to [their] operations or business arrangements; or any other circumstances that [they] know or have reason to know may have a material impact on [their] information security program.

To meet this requirement, institutions should undertake regular risk assessments. Large organizations should ensure that these assessments are coordinated across the enterprise. To ensure that the organization's security program adequately supports its privacy objectives and related information management controls, the security assessments should be combined in practice with privacy compliance and impact assessments. Smaller organizations may be able easily to integrate these two types of assessment, as well as the implementation and management of their GLBA compliance processes.

Conclusion

The FTC safeguards rule becomes effective in May 2003, with a two-year grandfathering for review of service providers. Organizations should not just assume that they meet the FTC safeguards rule simply because they have a security program or have in the case of smaller organizations taken steps to implement security measures that are consistent with industry practices. While the FTC is not, like the banking agencies, authorized to conduct compliance audits, the commission will look toward means of enforcement. For example, where a security breach has triggered a deceptive trade practices enforcement because of representations made in a privacy notice, as in the Eli Lilly example, the commission may look at all of the components of the security program as well as those indicated as the cause of the privacy violation. Rather organizations should begin now to review their security programs with the objectives of the FTC safeguards rule in mind, and for larger organizations, to coordinate and integrate privacy and security management processes across the enterprise. ■

References

1. The guidelines do, however, permit a board to assign implementation responsibilities to a committee or individual.

About the author

Patrick F. Sullivan, PhD, is the vice president of privacy and information policy at Guardent and is the Financial Services editor of this newsletter. He can be reached at patrick.sullivan.com@guardent.com.

Directive

from page 1

wireless location data and phone directories.

Cookies

The new directive requires European Union member states to limit the use of "cookies" and other similar technologies to those circumstances where users are "provided with clear and comprehensive information … about the purposes of [their use] and is offered the right to refuse such processing." However, the directive exempts those cookies "strictly necessary in order to provide [a] service explicitly requested by the subscriber or user."

Cookies are small text files sent by Web servers to be stored on the hard drive of Web site visitors. These files often contain personalization setting or unique identifiers for use in tracking the movements of users within and between Web sites.

While the distinction between regular cookies and those deemed "strictly necessary" is not clarified in the directive, some commentators have suggested that the first portion of the directive applies to so-called "persistent" cookies while the latter verbiage may apply to "session" cookies whose usage is often required for complex e-commerce transactions but whose quick deletion makes them less of a privacy threat.

Persistent cookies are often used for tracking a user's interests or preferences over a prolonged period of time such as what Web pages the user has visited or which stock symbols a user prefers to view in the stock ticker on a financial Web site. Session cookies usually exist only for the duration of a user's activities on a Web site, and are often associated with tracking the contents of a shopping cart or designating to the Web server that a user has successfully logged in to a password-protected part of a Web site.

The text adopted by the European Parliament recognizes that cookies can be used for many legitimate purposes, therefore "their use should be allowed on condition that users and subscribers have access to clear and precise information about the purposes of cookies or similar devices ensuring that the user is aware of information being placed on the terminal equipment he is using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment." Currently, most commercially available Web browsers permit users to choose to accept or reject cookies.

In justifying this approach, the drafting committee stated that, "Cookies are legitimate tools which serve a range of useful purposes. By enabling Web site functions, cookies enhance surfing experience and provide for effective Web services. Clear and comprehensive information will enable consumers to make an informed choice." In practice, most sites will be expected to disclose the existence of cookies on a Web site in the site's privacy policy.

Spam

The new directive also prohibits the use of automated telephone dialers, fax machines, and electronic mail for direct marketing unless recipients have given their prior consent to receive solicitations through those channels. This amounts to an "opt-in" requirement on all unsolicited e-mail, often called "spam" from entities without an existing business relationship with the recipient.

For e-mail solicitations between companies and their customers, the directive establishes what has been called a "soft opt-in" approach. This approach permits companies that obtain e-mail addresses from customers during a transaction to use that e-mail address for subsequent marketing solicitations.

However, the directive requires that "customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of [their e-mail address] when they are collected and on the occasion of each message where the customer has not initially refused such use." In short, customers must be given a clear

*See **Directive**, page 6*

Enclaves

from page 8

and confidentiality requirement, the intrusion detection agent will satisfy the *anticipated threats* obligation, and the firewall will *protect against unauthorized access*. Figure 1 on page 8 illustrates this enclave process.

Conclusion

If the enclave model were extrapolated to encompass the entire organization, the level of security *and* privacy could substantially increase. For example, published reports confirm that the majority of breaches still occur from internal users rather than outside attackers. Because of its segregation and additional security, the enclave model could provide a stronger protection against internal threats. Additionally, recent Federal Trade Commission actions are directly tied to internal misuse of private data. The enclave model offers more localized control within the organization over the implementation of security policies and data management, thereby providing tighter accountability and mitigating against inadvertent violations of policy or disclosures of data.

By controlling internal access to regulated information through an enclave model, significant gains can be made in protecting private information from both intentional and unintentional disclosure. The enclave model thus offers a potentially strong option for institutions that are working to implement cost efficient and effective privacy and security management. ■

About the author

John J. Masserini, CISSP, is a senior principal consultant with Guardent's Enterprise Security and Privacy practice. He can be reached at John.Masserini@Guardent.com.

Directive

from page 5

opportunity to decline future solicitations, both at the time of data collection and in each subsequent message.

For other kinds of unsolicited marketing communications not otherwise addressed in this directive, the European Parliament chose to let individual member states make their own choice between "opt-in" and "opt-out" regimes. For example, an earlier proposed draft had specifically included a ban on unsolicited marketing via simple messaging systems (SMS), a feature of mobile phones that is growing in popularity in Europe. However the text adopted by the European Parliament omitted that language, presumably leaving the issue up to member states.

The directive goes on to prohibit "disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease." The use of false addressing information or disguised sources is a widespread practice of e-mail "spammers." This provision is similar to restrictions currently in force in more than a dozen states in the United States.

Although several anti-spam proposals have been debated in Congress since 1997, currently there is no federal anti-spam legislation in effect.

Other provisions of the directive deal with the compilation of subscriber directories by communications services, restricting the public availability of individuals' data only with express permission of each subscriber. The directive also sets limits on the collection and storage of location-based data gathered from mobile phones and other devices.

Early Reaction

Early public reaction to the European Parliament's action brought angry responses from direct marketers and cheers from privacy advocates. At present, very few major marketers use unsolicited commercial e-mail for advertising; however, opponents to the EU directive are concerned that future marketing opportunities will be lost under the EU's restrictions.

Direct marketing industry protests notwithstanding, the remaining guidelines do not appear to pose tremendous obstacles for those businesses operating under current industry best practices. At present, most major online marketers already adhere to industry self-regulatory guidelines that urge companies to give customers notice and choice regarding how their e-mail address and other data will be used.

Similarly, the online advertising networks that comprise the Network Advertising Initiative, members of which make extensive use of cookies for tracking consumers across the Web, have has already adopted self-regulatory guidelines requiring clear notice and choice whenever cookies are used. ■

About the author

Ray Everett-Church is with ePrivacy Group and is the Internet Section editor of this newsletter. He can be reached at ray@eprivacy.com.

New York Appellate Court Rejects Privacy Damage Allegations

Kirk J. Nahra

In an important decision for any company evaluating litigation risks related to privacy laws and regulations, an appellate-level court in New York has rejected a class-action complaint concerning a disclosure of customer information to telemarketing firms, in violation of the company's privacy policy, because no actual injury was suffered by the customers whose information was disclosed. This case has important implications for any company facing privacy litigation based on misstatements in privacy policies or other allegedly wrongful disclosures of personally identifiable information.

Customer Information Sales Challenged

In *Smith v. Chase Manhattan Bank*, 2002 N.Y. Slip Op. 03015 (April 15, 2002), the Second Appellate Department addressed a purported class action to recover damages for alleged violations of New York General Business Law section 349, which prohibits deceptive practices. According to the complaint, Chase violated its own privacy policies when Chase sold customer information to nonaffiliated third-party vendors, including the name, address, telephone numbers, and other personal information of the plaintiff and the other alleged class members. These customer lists were then provided to telemarketing firms and direct mail agencies, which used the information to conduct solicitations. In return for the customer information, Chase allegedly received a commission on products or services that were purchased.

In order to state a cause of action under the General Business Law, the plaintiff needed to allege that the challenged act was consumer-oriented, that it was misleading in a material way, and that the plaintiff suffered injury as a result of the deceptive act. The practices at issue must be "likely to mislead a reasonable customer acting reasonably under the circumstances." In addition, the plaintiff must establish actual injury, although this does not necessarily require pecuniary harm.

No "Actual Injury" Alleged

The court presumed that the allegations of the complaint were true and indicated that, if true, the allegation that Chase sold confidential customer information to third-party vendors in violation of its privacy policy did allege actionable deception. However, in the decision's dispositive holding, the court found that the plaintiffs "have not alleged, and cannot prove, any 'actual injury'" as required by the statute. According to the court, the "harm" at the heart of the purported class action "is that class members were merely offered products and services which they were free to decline. This does not qualify

as actual harm." Moreover, the court added that the "complaint does not allege a single instance where a named plaintiff or any class member suffered any actual harm due to the receipt of an unwanted telephone solicitation or a piece of junk mail." Accordingly, the court dismissed the complaint.

This decision creates significant opportunities for defendants that are threatened with class action litigation, but where no specific injury results from any alleged wrongful disclosure of personal information. In this court's view, the mere wrongful disclosure of information does not create actual injury. With the millions of privacy notices required by the Gramm-Leach-Bliley Act and forthcoming under the Health Insurance Portability and Accountability Act, can misstatements in these notices create any kind of actual injury for customers and others that receive these notices? This precedent will be useful not only in resisting class action status (the allegations of injury arguably need to be sufficiently individualized to prevent a class certification) but also on the merits of whether an actual injury has been alleged that can sustain a cause of action. As covered entities grapple with Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, and other privacy statutes and regulations, the *Smith* decision represents some good news for companies trying to meet their privacy compliance obligations. ■

About the author

Kirk J. Nahra is a partner with Wiley Rein & Fielding, LLP. in Washington, D.C., specializing in privacy and insurance fraud issues. He can be reached at 202/719-7335 or knahra@wrf.com.

Proposed Internet Radio Listener Log Scrapped

Lisa A. Dunner, Esq., and Thomas A. Harvey

Several months ago, the U.S. Copyright Office issued a notice of proposed rulemaking directed to the requirements for giving copyright owners notice of the use of their sound recordings and the procedure for recording such use. Specifically, the proposed rules required online music services to provide copyright owners notice and keep records when copyrighted works are streamed over the Internet. One feature of this proposal — the creation of "listener logs" — has now been scrapped due to privacy concerns.

Listener logs, part of a copyright royalty system proposed by the Recording Industry Association of America, were designed to give copyright owners reasonable notice of the use of copyrighted material. The feature would have required Internet audio services to record information about their users, including the music they select, the date and time of transmission, the country of transmission, and the time zone where the transmission was received. The logs also would have assigned every user a unique user identifier for each listening session.

Privacy advocates criticized listener logs as unnecessarily invasive on user privacy, leading the copyright office to reject further consideration of them. As a result, only the second feature of the proposed rules, which requires digital audio services to create "intended playlists," remains open for consideration. This feature would require digital audio services to track information such as the recording title, the featured artist, the album title, the recording label, the catalog number and, where available, the international standard recording code (ISRC).

While commentators criticized both playlists and listener logs as unduly burdensome on digital audio services, only listener logs drew fire from privacy advocates. The Electronic Frontier Foundation, Electronic Privacy Information Center, and several radio organizations filed a cooperative response warning that listener logs represented an unprecedented change in the privacy landscape facing music listeners and that they would contribute to the erosion of listener privacy. The group also noted that the decision to "gather and report 'listener-side' information" would be a departure from privacy expectations in traditional radio, where listeners are anonymous and neither broadcasters nor copyright owners know who is tuning in.

The EFF and EPIC also stated that listener logs could be used for "deriving personally-identifiable information regarding users, or otherwise building individual user profiles." For example, companies with listener-side data could "partner with streaming audio vendors (such as Real Networks or Microsoft) or others (such as Doubleclick) to profile individual users."

As a result of this heavy criticism, the RIAA withdrew its proposal for listener logs, and the copyright office followed suit by tabling any further discussion of them. The RIAA retracted its proposal because it heard overwhelming negativity regarding listener logs well before the final deadline for filing comments within the copyright office. The director of the copyright office, Marybeth Peters, confirmed in May that the listener log idea is now "off the books. It's over."

Nevertheless, privacy advocates are concerned about the future implications of the listener log proposal. EFF and EPIC comments warned that the general trend to increase record-keeping requirements, even if they did not include listener logs *per se*, would impose prohibitive costs on many digital broadcasters, ultimately causing decreased digital services. "This outcome harms everyone — copyright owners will be denied royalties, broadcasters will be unable to reach new listeners, and listeners will face a less diverse Internet music environment." ■

About the author

Lisa A. Dunner is senior counsel (ldunner@skgf.com) and **Thomas A. Harvey** is a summer associate with the intellectual property firm of Sterne, Kessler, Goldstein & Fox P.L.L.C. in Washington, D.C.

Ensuring Privacy through Secure Enclaves

Secure Architecture Designs that Enable Privacy

John J. Masserini

For years, security experts have been evangelizing the benefit of replacing the monolithic "go-everywhere-and-do-everything" network paradigm with one that is more activity focused and business-centric. By breaking up the wide area network into smaller, more manageable chunks, or enclaves, network and security administrators could tailor the authentication and authorization controls to the specific business needs while limiting the overall risk to the organization.

Recently however, the secure enclave effort has gained momentum as a way to satisfy several of the requirements set forth by the recent wave of privacy regulations. In this article we examine the potential benefits of secure enclaves and how they can address some of the privacy issues faced in today's networked environments.

The Ever-Expanding Network

The network environment has changed dramatically over the last several years. Where once it was the norm for organizations to be totally cut off from the outside, the opposite is the case today. Collaboration, outsourcing arrangements, and other types of business partner connections all have opened up the infrastructure to unknown, and untrusted, entities. Dedicated, persistent connections from external networks to a company's infrastructure potentially open channels for breaches in security and privacy that were never previously considered to be a threat.

With the varied and often uncontrollable aspects of business partner connections, coupled with the ongoing struggles of securing the infrastructure from insider threats, secure enclaves are getting more attention as a beneficial and cost-effective solution to security and privacy concerns. This can be especially important for financial services institutions that are outsourcing more technology functions and need to find effective ways to address Gramm-Leach-Bliley Act (GLBA) security guidelines.

Secure Enclaves — A Background

In general, *enclaves* are areas of the network that are segregated from the rest of the network for bandwidth, accessibility, or security reasons. For example, applications developers may have a small, segregated network that is cordoned off from the rest of the network to protect the production environment from untested code. Secure enclaves are areas of the network that are protected over and above the rest of the trusted network. This protection may include devices like firewalls or routers, strong authentication, or even fully encrypted network traffic. The process of determining the requirements of a secure enclave typically involves performing a risk analysis to identify the potential overall risk to the organization and protecting the enclave accordingly. This risk analysis, when incorporating the privacy requirements of an organization as they are supported by security policies and controls, could identify and facilitate the creation of "privacy enclaves" as a way to meet the goals and objectives of the company's privacy policies.

Privacy Enclaves — A Solution Whose Time has Come

Just as the need for additional security spawned the development of secure enclaves, the need for additional privacy controls on information use and disclosure is causing enterprises to evaluate the need for privacy enclaves. This is particularly the case in organizations with data that are regulated through required administrative policies that define business rules for information use and mandated frameworks for implementing appropriate security controls. For example, section 501(b) of GLBA calls for financial institutions to *insure security and confidentiality*, *protect against anticipated threats*, and to *protect against unauthorized access*. By leveraging an appropriately designed privacy enclave, a financial institution could meet the requirements of all three of these directives with a relatively negligible expense and resource expenditure.

For example, suppose that a privacy enclave could be developed that would segregate the account holder's information from the rest of the institution's user and server populations. The account holder enclave would be protected by a firewall, limiting access to the account holder information to only those authorized to have such access. If necessary, the traffic behind the firewall could be encrypted in addition to encrypting the records while in storage. Additionally, an intrusion detection system agent could be deployed to monitor access attempts to the information, alerting network administrators, and creating a log to document compliance efforts. If we again look at 501(b), the encryption will address the *security*

See ***Enclaves****, page 5*

Figure 1: Example Enclave Model