Privacy Principles for Accountants

Legal Issues and Business Opportunities

By Mary J. Hildebrand and Matthew Savare

Europe has taken an aggressive stance on protecting individual privacy with its comprehensive European Union Privacy Directive. The United States, however, has, until fairly recently, adopted a more *laissez-faire* approach. Over the last several years, there has been a dramatic increase in the incidents of identity theft and high-profile data security breaches—many involving accountants, tax preparers, and auditors. For example, in January 2006, some H&R Block clients' Social Security numbers appeared on mailing labels. Similarly, Deloitte & Touche, the AICPA, and even the IRS have also suffered from data breaches. In light of these problems, American consumers and legislators have begun to focus on the privacy of personal information.

Identify theft is the most rapidly growing white-collar crime (Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, January 2006). Surveys estimate that approximately 10 million consumers are victimized each year by some type of identify theft. The Federal Trade Commission (FTC) estimates that identity theft cost businesses approximately $50 billion in 2003 (Joel Winston, "Identify Theft and Social Security Numbers," *E-Commerce Law Report*, April 2006). In this environment, protecting consumer privacy is rapidly becoming one of the most significant legal and technological challenges facing businesses. Respecting and safeguarding consumer privacy is not just a legal issue, however. It is also a business issue that can profoundly impact a company's risks, reputation, and bottom line.

Legal and Compliance Issues

Privacy, a vague, abstract concept, means different things to different people. It is one aspect of disparate legal issues such as abortion, wiretapping, airport screening, disclosure of medical or financial information, police searches, and journalism. Solove's article quoted one privacy scholar's lament: "Privacy seems to be about everything, and therefore it appears to be nothing."

This article uses the AICPA's definition of "privacy" as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information." Viewed in this context, CPAs need to comply with a host of information privacy laws, regulations, and rules.

Gramm-Leach Bliley Act. The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA; 15 USC sections 6801–6809), and its accompanying FTC regulations govern the collection, use, disclosure, and protection of consumers' "nonpublic personal information." 16 CFR section 313.3(n)(1) defines "nonpublic personal information" as "(i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available." GLBA applies to "financial institutions" that are "significantly engaged" in providing individual clients with "financial products or services" for personal, familial, or household purposes (i.e., nonbusiness purposes). Significant for accountants, the statute covers the preparation of individual tax returns and the provision of nonbusiness tax or

financial planning advice. As such, accountants who provide these types of services to individual clients must comply with GLBA.

GLBA imposes two significant requirements upon accountants who are covered by the statute. First, accountants are prohibited from disclosing to a nonaffiliated third party any nonpublic personal information of their clients, such as Social Security numbers, tax return data, and account information (15 USC section 6802). GLBA does permit "financial institutions" to disclose certain information if a client is provided an opt-out notice and a reasonable opportunity to opt out of the disclosure. As noted later herein, IRC section 7216 restricts accountants' use and disclosure of clients' federal tax return information. Furthermore, FTC staff has stated unequivocally of the GLBA's exemption: "The Privacy Rule does not supersede the restrictions in section 7216. The GLB Act and the Agencies' implementing regulations do not authorize a financial institution to disclose nonpublic personal information in a way that is prohibited by some other law. Therefore, you may not avoid the restrictions of section 7216 by providing your customers with an opt-out notice and a reasonable opportunity to opt out" (FTC, "Frequently Asked Questions for the Privacy Regulation," www.ftc.gov/privacy/glbact/glb-faq.htm#A) Disclosure is permitted, however, to effect or administer a client transaction (e.g., disclosure of a tax return to a tax return processor); to participate in a peer review; to comply with federal, state, or local laws; and to comply with court orders.

Second, FTC regulations require accountants to "develop, implement, and maintain a [written] comprehensive information security program" that outlines the ways in which they protect client information (16 CFR section 314.3). The program must be tailored to the size and complexity of the accountant's practice, the nature and scope of the services, and the sensitivity of client data. As specified by 16 CFR section 314.4, under the security plan accountants must do the following:

- Designate the employees to coordinate the safeguards;
- Identify and assess risks to customer information;
- Create, monitor, and test a safeguards program that addresses the risks identified during the assessment;
- Select appropriate service providers and require them by contract to implement these safeguards; and
- Evaluate the plan and adjust it as necessary.

Because AICPA Code of Professional Conduct Rule 301 mandates that "[a] member in public practice shall not disclose any confidential client information without the specific consent of the client," the safeguards program should not require accountants to perform many additional tasks. At minimum, accountants should document their existing safeguard plan, designate someone to coordinate it, and require their service providers to comply. Requiring service providers to agree to safeguard client data comports with the recommendations outlined in AICPA Rule 391, which states: "[T]he member should enter into a contractual agreement with the third-party service provider to maintain the confidentiality of the information and be reasonably assured that the third-party service provider has appropriate procedures in place to prevent the unauthorized release of confidential information to others."

With more tax-return preparation work being sent overseas, accountants must recognize that although they can outsource certain job functions, they cannot outsource their legal liability for privacy violations. According to Amy E. Yates ["Sit, Walk, Heel, Stay (or How to Train Your) Outsourcer," *SciTech Lawyer*, Summer 2006], privacy experts recommend that covered entities such as accountants employ six rules to meet their obligations under data privacy laws and to manage their risks when outsourcing to third parties:

- Enter into a contractual agreement with the third party that delineates that party's specific obligations, rather than simply stating that the party will comply with all applicable laws and regulations.
- Perform a "gap" analysis and determine if the third party's privacy and security policies are adequate.
- Become familiar with the third party's processing practices. For example, is the third party collecting more confidential information than is necessary to complete the required job?
- Perform privacy audits on the potential and existing outsourcers on a periodic basis.
- Establish a strong working relationship with the vendor's chief privacy officer.
- Employ and maintain strong privacy protections in the accounting firm.

Prior to October 13, 2006, GLBA required accountants to provide annual notices to clients regarding their privacy policies. On that date, President Bush signed into law the Financial Services Regulatory Relief Act of 2006, which contained a provision exempting CPAs from this requirement ("President Bush Signs into Law Bill Giving CPAs Exemption from Gramm-Leach-Bliley Annual Notification Requirement," www.aicpa.org/pubs/cpaltr/nov2006/story2_nov06.htm).

Notwithstanding this exemption, the AICPA still strongly recommends that accountants maintain and enforce a privacy policy. The privacy policy does not need to be personalized for each client. Instead, it can be posted to the accountant's website or provided in conjunction with a bill, engagement letter, or newsletter. The policy, which should be clear, conspicuous, and accurate, should describe the following items:

- Types of nonpublic personal information the accountant collects;
- Types of such information that the accountant discloses;
- Parties to whom the accountant discloses such information;
- Circumstances under which the accountant discloses such information;
- The policy regarding sharing information of former clients; and
- The practices for protecting such information.

An accountant who drafts and disseminates a privacy policy should comply with it. A breach of a privacy policy, even an unintentional one, can expose the accountant to claims of breach of contract, negligence, or unfair and deceptive trade practices.

IRC and Treasury regulations. IRC section 7216 prohibits tax preparers from "knowingly" or "recklessly" disclosing or using tax-related information other than in connection with the preparation of the return. The statute provides for fines and possible imprisonment for such viola-

tions. Disclosures pursuant to a court order or to third parties assisting in the processing of the return are permissible. Currently, there are no requirements to inform a client that a third-party provider, including an overseas provider, is being used. Similarly, IRC section 6713 imposes a $250 civil penalty for each improper use or disclosure of client information, with the total penalty not to exceed $10,000 for any person for a calendar year.

Treasury Department regulations enacted pursuant to the IRC permit accountants to disclose or use tax return information for three discrete reasons, provided the client signs a formal written consent (26 CFR section 301.7216-3). First, the regulations permit accountants to use tax return information to solicit from their clients additional non-IRS services that they provide to the general public [26 CFR section 301.7216-3(a)(1)]. The regulations provide three examples of when such a consent is required [see 26 CFR section 301.7216-3(c)]. Examples of such services include refund anticipation loans, balance due loans, mortgage loans, mutual funds, IRAs, and life insurance. The request for this type of consent must be made before the taxpayer receives his completed return, and if the taxpayer refuses to give consent, no follow-up request may be made. Second, the regulations allow accountants to disclose tax return information to such third parties, including marketers, as the taxpayer may direct [26 CFR section 301.7216-3(a)(2)]. Finally, with the proper consent, accountants may disclose or use the tax return information from one client to aid in the preparation of a tax return for another client [26 CFR section 301.7216-3(a)(3)].

As provided for by 26 CFR section 301.7216-3(b), the accountant must obtain a separate written consent signed by the client for each separate use or disclosure. The consent must contain the following information:

- Name of the tax return preparer;
- Name of the taxpayer;
- Purpose for which the consent is being furnished;
- Date on which such consent is signed;
- Statement that the tax return information may not be disclosed or used by the tax return preparer for any other purpose; and
- Statement by the taxpayer that he consents to the disclosure or use of such information for the specified purpose.

In December 2005, the IRS issued proposed amendments to 26 CFR section 301.7216 (Department of the Treasury, "Guidance Necessary to Facilitate Electronic Tax Administration—Updating Section 7216 Regulations," December 8, 2005). The proposed changes included broadening the definitions of "tax return preparer" and "tax return information"; revising the manner and form of obtaining client consent to use or disclose tax return information; and introducing a new requirement to obtain taxpayer consent before sending any tax return information outside the United States, including to subcontractors doing the actual tax preparation. The IRS's proposed wording for consents to disclose and to use tax information stated the following:

> We generally are not authorized to disclose your tax return information for purposes other than the preparation and filing of your tax return. We may disclose your tax return information to third parties only if you consent to each specific disclosure. Your consent is valid for one year.
>
> **Warning:** Once your tax return information is disclosed to a third party per your consent, we have no control over what that third party does with your tax return information. If the third party uses or discloses your tax return information for purposes other than the purpose for which you authorized the disclosure, under Federal tax law, we are not responsible for that subsequent use or disclosure, and Federal tax law may not protect you from that disclosure.
>
> We generally are not authorized to use your tax return information for purposes other than the preparation and filing of your tax return. We may use your tax return information for other purposes only if you consent to each specific use. Your consent is valid for one year.

As of the publication of this article, these proposed changes have not been adopted. Indeed, many experts, including William Stromson, the AICPA's director of taxation, believe that Congress will petition for even greater privacy protections, including a possible outright prohibition from sharing a client's tax return information, even with formal, written consent.

Individual states' privacy laws. Federal privacy legislation tends to focus on specific economic sectors, such as the financial industry, which is regulated by the privacy and security provisions of GLBA. Nevertheless, state data-security laws typically extend beyond particular industries. For example, as of January 2008, at least 39 states and the District of Columbia have enacted security breach notification laws that impose security and privacy standards that are generally applicable across industries (National Conference of State Legislatures, "State Security Breach Notification Laws," www.ncsl.org/programs/lis/cip/priv/breachlaws.htm). These states include California, Florida, New Jersey, New York, and Texas (see David Leit and Matthew Savare, "New Jersey Enacts Identity Theft Prevention Act," *The Metropolitan Corporate Counsel*, February 2006). CPAs are well advised to research whether their state has passed additional privacy legislation that could impact their business operations.

One example of this type of legislation, New Jersey's Identity Theft Prevention Act, requires businesses to notify New Jersey consumers if their personal information has been compromised; requires businesses and public entities to thoroughly destroy customer records that are no longer to be retained; and limits the use and display of Social Security numbers.

Facing these statutory requirements and similar laws from other states, accountants should take the following measures to mitigate their risks:

New Jersey's Identity Theft Prevention Act requires businesses to notify consumers if their personal information has been compromised, and requires businesses and public entities to thoroughly destroy customer records that are no longer to be retained.

■ Adopt and implement robust electronic and physical safeguards to protect and monitor clients' personal information. For example, all filing cabinets containing tax-related information should be locked, and all computers, laptops, and networks should be password-protected. Electronic data, particularly data stored on laptops and networks, should be encrypted using industry-standard protocols (i.e., 128-bit secure socket layers). Laptops are especially vulnerable. A 2006 survey report indicated that 81% of the companies questioned reported the loss of at least one laptop containing sensitive data during the past 12 months (David Lazarus, "Data Theft May Hurt Workers," www.sfgate.com).

■ All paper and electronic files that are to be discarded should be obliterated. Paper documents should be cross-shredded or destroyed by a third-party vendor that specializes in document destruction. Floppy disks should be thoroughly destroyed, not simply erased or reformatted. Similarly, before an old computer is discarded or sold, its hard drive should be removed and then either physically destroyed beyond reconstructability, or encrypted and then permanently stored. No deletion, reformatting, or wiping function can completely guarantee that a hard drive has been stripped of all confidential information (David Beckman and David Hirsch, "Hard Drive Homicide: Old Hard Drives Must Rest in Pieces for Lawyers to Truly Rest in Peace," *ABA Journal,* August 2006).

■ Whenever possible, employ the principles of "data minimization" and "retention limitation." The former means that "unneeded data is not collected in the first place." The latter means that "data that is outdated or no longer needed is securely and effectively deleted or destroyed" (Ann Cavoukian, "Fighting Identity Theft Starts with Businesses, Not Consumers," *SciTech Lawyer*, Summer 2006). Accountants should not be overzealous in practicing this "retention limitation," however, because IRC section 6107(b) requires them to retain copies of completed tax returns or maintain a list of all returns, including clients' names and Social Security numbers, for three years after the close of a return period.

Business Opportunities

Privacy is a risk-management issue for businesses. Conceptualizing, implementing, monitoring, and enforcing strict privacy safeguards are instrumental in reducing such privacy-related risks as identity theft, extortion, litigation, lost business, and a reduced stock price. Moreover, enhancing privacy protection protects valuable business assets, preserves and enhances a company's brand and reputation, and preserves and augments customer loyalty. Accordingly, businesses, particularly those with an online presence, have retained privacy lawyers and information consultants to address their privacy needs. Increasingly, businesses are also engaging accountants for a broad array of privacy services.

Accountants are well advised to consult with an experienced privacy attorney before offering privacy services to the public.

Accountants possess the technical skills and training to provide information assurance, compliance testing, independent verifications, and attestations of management reporting. Historically, accountants have provided these services as they relate to financial reporting. With the current emphasis on information privacy, many accountants now offer the following privacy services as well:

■ Strategic privacy and business planning
■ Privacy gap and risk analysis
■ Benchmarking
■ Privacy-policy design and implementation
■ Performance measurement
■ Independent verification of privacy controls (privacy audits)
■ Attestation of management's privacy reports.

As noted above, privacy legislation is a patchwork of federal and state statutes and regulations. As such, accountants are well advised to consult with an experienced privacy attorney before offering privacy services to the public. At minimum, however, accountants should have at least a rudimentary independent understanding of the following privacy statutes:

Health Insurance Portability and Accounting Act (HIPAA). HIPAA [PL 104-191, 110 Stat. 1936 (1996)] and the regulations promulgated under it are the first set of comprehensive rules on health privacy. However, these regulations do not apply to all people or entities that have access to an individual's health information. Instead, they apply only to "a health plan," "a health care clearinghouse," and "a health care provider who transmits any health information in electronic form" (45 CFR section 160.102). These "covered entities" are defined in 45 CFR section 160.103 as follows: a "health plan" is "an individual or group that provides, or pays the cost of, medical care." This definition encompasses health insurers, HMOs, and group health plans. A "health care clearinghouse" is a public or private entity that processes health information into a standard format or into specialized formats for the needs of specific entities. This definition includes billing services, repricing companies, community health management information systems, and community health information systems. Finally, a "health care provider" is a "provider of medical or health services … and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." Examples of healthcare providers include physicians, hospitals, and pharmacists.

HIPAA's privacy rule creates standards for electronic transactions, data security, patient identification numbers, and the privacy of health information.

Gramm-Leach Bliley Act (GLBA). As discussed in detail above, GLBA applies to "financial institutions." The statute governs privacy issues for personal financial information.

Children's Online Privacy Protection Act (COPPA). COPPA (15 USC sections 6501–06) regulates the collection and use of children's information by websites. It applies to "an operator of a website or online

service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child."

Important elements of COPPA include: 1) a requirement that children's websites post their privacy policies, describing "what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information"; 2) a requirement that operators of such sites "obtain verifiable parental consent for the collection, use or disclosure of personal information from children"; 3) a prohibition of websites conditioning a child's participation in a game or receipt of a prize on the disclosure of more personal information than is necessary to participate in that activity; and 4) a requirement that operators of such sites "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM). The CAN-SPAM Act establishes requirements for those who send commercial e-mails, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them. The law has four significant components:

- It bans false or misleading header information. The "To," "From," and routing information—including the originating domain name and e-mail address—must be accurate and identify the person who initiated the e-mail.
- It prohibits deceptive subject lines (i.e., the subject line cannot mislead the recipient about the contents or subject matter of the message).
- It requires that the e-mail provide recipients with an opt-out method. In other words, the sender must provide a return e-mail address or another Internet-based response mechanism that allows a recipient to ask the sender not to send future e-mail messages to that e-mail address. Once the sender receives such an opt-out demand, it must honor the request within 10 business days. In addition, the sender cannot help another entity send e-mail to that address or have another entity send e-mail on its behalf to that address.
- It requires that commercial e-mail contain a clear and conspicuous notice that the message is an advertisement or solicitation and must include the sender's valid physical postal address.

Federal Trade Commission Act (FTC Act). Since 1998, the FTC has been suing companies that violate their own privacy policies (Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004). These actions are brought under the FTC Act (15 USC section 45), which prohibits "unfair or deceptive" business practices. The FTC has interpreted this statute as being violated when a company breaks the promises it makes in its privacy policy.

AICPA's "Generally Accepted Privacy Principles: A Global Privacy Framework." Most companies are not legally required to maintain a privacy policy. As discussed above, "financial institutions" covered by GLBA, "covered entities" governed by HIPAA, and websites directed at children that fall under COPPA are all required to maintain and enforce a privacy policy. However, most companies do so because consumers have come to expect some type of written privacy policy, especially from online retailers. If a business opts to have a privacy policy, then it must comply with its provisions or it risks facing an FTC action or a breach-of-contract lawsuit. The AICPA has developed "Generally Accepted Privacy Principles: A Global Privacy Framework" (infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles.htm), which is an invaluable resource for accountants to address the privacy-compliance issues of their clients, including drafting and enforcing privacy policies.

The AICPA states that the framework's privacy objective is that: "Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA/CICA [Canadian Institute of Chartered Accountants]." Page 7 of the document lists 10 "Generally Accepted Privacy Principles" and provides objective, measurable criteria against which accountants audit each of the principles:

- Management: "Entity defines, documents, communicates, and assigns accountability for its privacy policies, and procedures."
- Notice: "Entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed."
- Choice and consent: "Entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information."
- Collection: "Entity collects personal information only for the purposes identified in the notice."
- Use and retention: "Entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes."
- Access: "Entity provides individuals with access to their personal information for review and update."
- Disclosure to third parties: "Entity discloses personal information to third parties only for the purpose identified in the notice and with the implicit or explicit consent of the individual."
- Security: "Entity protects personal information against unauthorized access (both physical and logical)."
- Quality: "Entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice."
- Monitoring and enforcement: "Entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes."

CPAs seeking to provide privacy advisory services are well advised to counsel their clients to employ the framework's 10 privacy principles. In addition, they should consider using the objective criteria in the framework when evaluating an entity's privacy policies, procedures, and controls. ❑

Mary J. Hildebrand, Esq., *is a senior member of Lowenstein Sandler, PC. She can be reached at mhildebrand@lowenstein.com.* ***Matthew Savare, Esq.,*** *is an associate, also of Lowenstein Sandler, PC. He can be reached at msavare@lowenstein.com.*