

Current Privacy Legislation in the US

a report by

Jan Lovorn

Chair, Policy and Privacy Working Group, PKI Forum

The landscape of personal information and its protection is changing in parallel with the changes in the ability for people and businesses to collect, generate, process and share information. Many people can remember when computers did not talk to each other and that information that was to be shared had to be placed on portable media with control and management by people.

Today, people e-mail or send instant messages to each other with documents, photos and other private exchanges. Businesses gather from, and consumers provide information through, the Internet, phone calls and hard-copy inputs, such as loan applications or product warrantee registrations, as well as share information that is collected automatically as they make supermarket purchases or view Web pages. Most people in the US have access to computers and the Internet. Information is collected about all facets of people's lives. For example, the *Wall Street Journal* reports that Time Warner has the names, addresses and information on the reading and listening habits of 65 million households.

Consumers and privacy advocates have expressed concerns about aggressive intrusions into people's private lives and the misuse of their personal information. Often, a consumer is required to provide personal information to obtain products or services. Many times, without the consumer's knowledge, information that is provided for one purpose is used for another. Financial institutions, Internet services companies, marketers and government agencies have acknowledged crossing the line.

Some members of Congress have been shining the spotlight on the protection of information, but are also working on ensuring that consumers are told about how and why personal information is collected and used, are provided with access to that data and given a choice in that matter. Legislation has been enacted in the US and other countries that sets requirements for privacy, including notice, consent and other key privacy requirements. However, as in all great trends in the marketplace, technology often outstrips the ability of public policy to keep pace with consumer and citizen expectations.

According to a Forester Research survey of online users, 67% stated that they were "extremely" or very concerned about releasing personal information over the Internet. Last year, a *Business Week*/Harris poll showed that 92% of Internet users are uncomfortable about websites sharing personal information and 57% favour the government passing laws on the way in which personal information is collected and shared. What this has led to on the consumer's side is that they sometimes provide false personal information to obtain the product or service that they want.

Financial Information Protection

Major new legislation affecting financial institutions is the *Gramm-Leach-Bliley Act 1999* (GLB). It states that financial institutions must safeguard personally identifiable financial information. Regulatory agencies must develop the detailed requirements on protecting this information. Key provisions of the act and of the regulations will be described as follows.

The GLB establishes extensive new obligations and rights with respect to consumer financial privacy. In general, it requires disclosure of policies and practices regarding disclosure of private financial information; prohibits the disclosure of private financial information to unaffiliated third parties, unless consumers are given the right to 'opt out' of such disclosure; and requires the establishment of safeguards to protect the security and integrity of private financial information. GLB applies to a broad range of financial institutions. It sweeps within its coverage not only traditional banks, security companies and insurance companies, but also all other providers of financial products and services as defined under Section 4 (k) of the *Bank Company Holding Company Act*. As a result, retailers issuing credit cards, money transmitters, cheque cashers, mortgage brokers, real-estate settlement services, appraisers, tax preparation services and online companies that offer aggregation, funds transfer or payment services are all under GLB.

Under this legislation, no company providing financial products or services to individuals for personal family or household purposes may give non-public information about those individuals to a non-affiliated

Jan Lovorn is Chair of the Policy and Privacy Working Group for the PKI Forum. She is the Chief Privacy Officer at Protegrity, a data-privacy technology vendor. She has over 20 years of experience in the information technology (IT) environment. This includes a broad IT-engineering background, with an in-depth knowledge of industry security standards, focusing on the expanding use of data-protection technologies and their implications on enterprise integration and business processes. She has guided standards development in support of several vendors and has testified on numerous occasions to the National Committee on Vital and Health Statistics of Health and Human Services. She is past Chairperson of the American Society of Testing and Materials (ASTM) 31.20 Data and Systems Security for Health Information and has been a member of the Financial Services-Data Security (X9.F1) Working Group on Cryptographic Tools and of the Financial Services-Data Security (X9.F3) Working Group on Cryptographic Procedures. Ms Lovorn is also a member of the US Technical Advisory Group (TAG) for the International Organization for Standardization (ISO) Technical Committee (TC) 215 on Health Informatics.

third party for any purpose outside of a specific list of exceptions without first giving the individuals the chance to opt out of that disclosure of information.

In addition, at the time of establishing a retail customer relationship with an individual, and at least yearly thereafter for the entire life of that relationship, a financial institution must provide the customer with a clear and conspicuous disclosure of the institution's policies and practices with respect to the disclosure of the collected or generated personal information to both affiliates and non-affiliated third parties.

These statutory requirements are implemented by regulations that have been adopted by seven federal agencies, including the bank supervisory agencies, the Securities and Exchange Commission and the Federal Trade Commission, as well as by rules that have been adopted in the US for insurance companies. Financial institutions were required to be compliant by 1 July 2001. Auditing for compliance is expected to begin in the September 2001 timeframe.

The key proviso for the privacy of the personally identifiable information is the new operational requirements for financial institutions to safeguard the personal information of consumers. The regulations under the statute are required to include appropriate standards for financial institutions relating to administrative, technical and physical safeguards to ensure the safety and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security and integrity of such records and to protect against unauthorised access to or use of such records or information. Details of these safeguards have been left to be implemented by the authority agencies.

Health Information Protection

Security and privacy are integral parts of the *Health Insurance Portability and Accountability Act 1996* (HIPAA). HIPAA aims to reform the insurance market and simplify healthcare administrative processes. HIPAA impacts any healthcare organisation that maintains or transmits electronic health information.

One of the goals of HIPAA's Administrative Simplification (AS) provision is to increase the use and efficiency of the electronic exchange of standard healthcare information. In order to achieve this, the security and confidentiality of electronic health information, i.e. medical records, billing, clinical results and insurance coverage, must be protected as specified in the security and the privacy regulations that have been developed as a result of HIPAA's AS provision.

The final privacy regulations were issued in April 2001 with implementations required in April 2003

with some delays to October 2003. The regulation is simple. The requirements include the following.

- Patients are told in plain English how their medical information is used, kept and disclosed.
- Patients are allowed to see their medical records and obtain copies of those records if desired. Patients are allowed to have inaccurate information corrected.
- Patients are allowed to consent to the disclosure of their health information in most circumstances, including for non-medical or non-treatment-related purposes.
- Rule limits the use of the information for health purposes with only a few exceptions.
- Healthcare organisations must adopt privacy procedures, train employees in them and provide a process if those procedures are violated.
- Hospitals and healthcare providers are held accountable if patient information is misused.
- Rule requires only reasonable safeguards to be used.
- Rule is flexible. People will still be allowed to pick up prescriptions for family members.
- Rule allows information sharing for treatment purposes.

HIPAA's security standards, which provide a base-line for establishing a security program, are comprehensive in order to avoid piecemeal implementation. Specific technologies are not required or promoted in the standards to provide the flexibility to take advantage of a future state-of-the-art technology. The standards are scalable so that they can be implemented by an organisation of any size. It does not address the extent to which a particular entity should implement the specific features. The standard stipulates a general set of practices. It is up to each organisation to assess its own security needs and risks, as well as to develop and document a security program that best fits those needs.

The proposed HIPAA security standard is divided into categories. Final regulations are due out before the end of 2001 with implementation in 24 months. They will include requirements for the following areas:

- administrative procedures – include documented formal practices for creating and enforcing security policies;
- physical safeguards – include documented processes for physically securing computer systems and related equipment and buildings; and

- technical security services – include documented technology and processes to protect, control and monitor information access.
- with certain exceptions, obtain verifiable parental consent before collecting, using or disclosing personal information from children; and

While technology is a significant part of HIPAA, the non-technical aspects of the law are equally significant. Healthcare-related organisations must examine and potentially modify business practices, document policies and procedures and send these to employees, vendors, contractors, business partners and patients through on-going, consistent training and security awareness programs.

Children’s Information Protection

The *Children’s Online Privacy Protection Act 1999* (COPPA) applies to operators of commercial websites and online services that are directed at children under the age of 13, where personal information is collected. The rule also applies to operators of general interest sites with actual knowledge that they are collecting information from children under the age of 13. Implementation of COPPA was required by April 2000. Those operators covered by COPPA must:

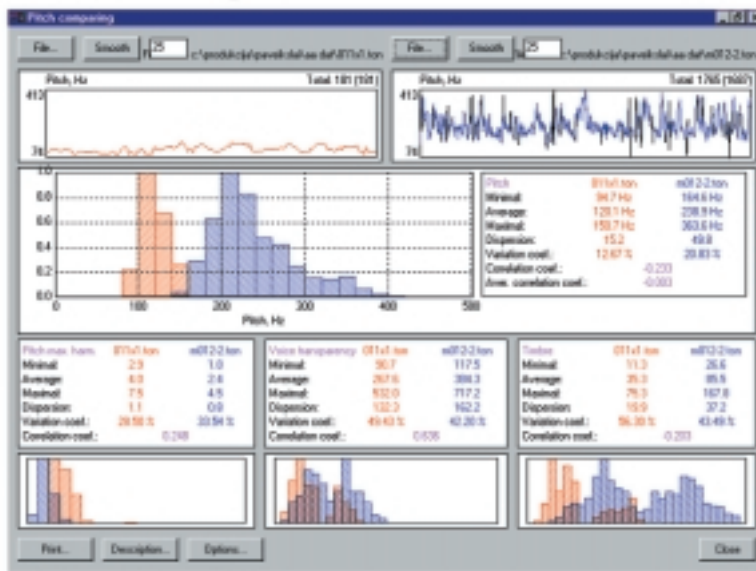
- post a privacy policy and links to the policy;
- give parents notice of its information practices;

- provide parental access to information that is collected from children and the opportunity to delete such information and to opt out of future collection.

Attempts to research or glean personal information should not be disguised as entertainment and prizes should not be used to induce children to provide personal information. COPPA requires organisations to provide a foolproof way in which to communicate directly with parents rather than rely on the children obtaining permission to access a website.

Pending or Planned Legislation

In the 107th Congress, more than 26 pieces were or will be proposed to protect US consumer’s private information gathered through providing financial services, healthcare and information delivery. The areas of new legislation include the protection of Internet users, medical financial information and personal information that can lead to identity theft. The implementation of legislation must balance privacy and access for both consumers and businesses. ■



**We have created
Technology
transforming your
Voice into a Key ...**