

The Race to Protect *Personal Information*

by Melanie C. Holloway and Janet P. Peyton

The concept of a “right to privacy” has been enshrined in state statutes and case law for decades. A constitutional right to privacy is rooted in the penumbra of the Bill of Rights.¹ The concept of privacy in our personal lives—to make personal choices about religion, education, marriage or contraception—is probably considered the most fundamental “right to privacy” today. Early privacy concerns focused on keeping the government out of our bedrooms and passersby from peeping through our window blinds.

Over time, many states, including Virginia, had statutes to protect commercial aspects of privacy. The focus of these laws, however, was to give individuals the right to prevent their names or likenesses from being used to advertise goods or services without the individual’s permission. Privacy laws were not typically designed to protect consumers from crime or to prevent unwanted distribution of contact information for marketing purposes.

Over the past 20 years, however, the value of personal data for both criminal and commercial purposes has grown exponentially, and entrepreneurial businesses (legitimate and otherwise) have taken advantage of the absence of laws in this area to capitalize on the availability of valuable data assets. State legislatures and the federal government continue to play catch-up as they try to protect consumer information without placing an undue burden on commerce. This article will survey existing privacy laws at the federal level and in Virginia and will discuss proposed

and pending legislation that likely will change the face of privacy law.

Federal Privacy Laws and Regulations

Although no one federal agency is tasked with enforcement of privacy laws, the mission of the Federal Trade Commission (FTC) in preventing the use of deceptive practices in commerce² has created a nexus between the agency and privacy issues. In the late 1990s, as companies rushed to have a presence on the World Wide Web, many Web site owners created what they called “privacy policies” to bolster consumer confidence in the security of information shared over the Web. The FTC began reviewing the published “privacy policies” of online Web site owners in an effort to root out deceptive practices. In doing so, the FTC developed five principles to be applied in evaluating privacy practices:

- **Notice**—A company should develop a clearly written, understandable privacy policy that explains its information practices.
- **Consent**—Consumers should be given options regarding the use and disclosure of their personal information.
- **Access**—Consumers should be able to access the personal information collected about them, as well as have the ability to modify this information or request that it be deleted.
- **Security**—Companies should use appropriate measures to protect the security of personal information they collect.

- **Enforcement**—Appropriate enforcement mechanisms must exist to ensure compliance with these principles.

Other major federal legislation enacted in the past 10 years was directed at specific kinds of information deemed to be extremely sensitive. For example, the Children’s Online Privacy Protection Act (COPPA), enacted in 1998, was a response to the surge in use of the Internet by children and concerns about their vulnerability. Similarly, the Financial Modernization Act of 1999 (better known as the Gramm-Leach-Bliley Act) was intended to protect sensitive financial information; it required financial institutions to be transparent with consumers about how financial information will be used, protected and, if necessary, disclosed. The spirit of the act is similar to the five principles used by the FTC to assess online privacy policies. The laws are less focused on what can be done with the information and more focused on disclosure to the owner of the data about the actual practices of the company, so that the consumer can make educated choices about use of data.

The Do-Not-Call Registry and CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act signaled a return to the concept of physical privacy. These laws give consumers tools to keep telemarketers at bay and to stop unsolicited e-mails that clog our inboxes. As concerns about protecting personal data continue to evolve, however, there is a push to regulate how the information is obtained and when and how it can be used.

Proposed Federal Privacy Legislation

Most existing federal privacy law is focused on protecting a specific category of personal information, such as medical (Health Insurance Portability and Accountability Act, or HIPAA), financial (Gramm-Leach-Bliley Act), children's (COPPA), or e-mail addresses (CAN-SPAM Act). Recently, however, the trend toward sweeping legislation to protect anything labeled "personal" has become pronounced. The proposed legislation falls into several categories. One is commonly referred to as "breach notification" legisla-

"Major security breach" is defined as a breach that impacts 10,000 or more individuals or any security breach of federal government databases.

tion. The objective of these kinds of laws is to require companies that experience a breach of security that results in possible disclosure of consumer data to take steps to notify those consumers so they can protect themselves from identity theft. One of the most significant pending proposals at the federal level is the Notification of Risk to Personal Data Act of 2007 (S. 239). The bill, re-introduced in 2007 by Senator Dianne Feinstein (D-California), would require not only notification of a data security breach to the affected individuals themselves, but also credit agencies for breaches affecting more than 1,000 individuals; the media, for breaches affecting more than 5,000 individuals; and the U.S.

Secret Service, for breaches affecting more than 10,000 individuals.

In the House of Representatives, a proposal by Representative Lamar Smith (R-Texas) would criminalize the intentional withholding of information about major security breaches. His bill, the Cybersecurity Enhancement and Consumer Data Protection Act, would provide for up to five years in prison for knowingly failing to provide notice to either the FBI or the Secret Service regarding a major security breach with the intent to prevent, obstruct or impede a lawful investigation of such breach. "Major security breach" is defined as a breach that impacts 10,000 or more individuals or any security breach of federal government databases.

Virginia Privacy Law

Like early federal legislation, the first Virginia privacy laws that affected data protected highly sensitive information, such as medical, court, tenant and insurance records.

Proposed Virginia Legislation

More recent Virginia privacy legislation has focused on fraudulent or otherwise improper methods of obtaining or using all personal identifying information. "Peeping Toms" invade our privacy by catching glimpses of our account, personal identification or credit card numbers, or passwords, as they travel the information superhighway. The absence of legislation to protect consumers from such invasions may simply be a case of leaving the blinds open.

In 2007, a number of bills were proposed in the General Assembly to address the identity-theft dilemma—both prevention (record disposal) and remediation (breach notification and credit freezes).

Disposal of Records

House Bill 2600 included a proposal to add protection under the Virginia Consumer Protection Act³ by prohibiting unauthorized access to or use of personal information contained in discarded records. The proposed legislation identi-

fied "reasonable measures" that businesses must take after disposal of records, including burning and shredding documents and destroying or erasing electronic and other nonpaper media.⁴

Breach Notification

The General Assembly was unable to pass breach notification legislation this year, despite numerous attempts. With some minor variations, each bill required a person or entity whose information system has been breached, resulting in unauthorized disclosure of personal information, to notify law enforcement, the Virginia resident whose personal information was accessed, and the Virginia attorney general's office.

The bill⁵ proposed in the House required *immediate* notification to a Virginia resident whose personal information has been accessed, or is reasonably believed to have been accessed, as a result of a breach in the security of an individual or commercial entity's system. Although the proposed law required immediate notification to the affected Virginia resident, it allows for a reasonable delay if law enforcement determines that notification will impede a criminal investigation.

If a company's own breach-notification policies and procedures are consistent with the timing requirements of the proposed law, then the company is deemed in compliance, provided that it complies with its own policy.

The bill provided a private right of action for Virginia residents, including mandatory award of treble damages and attorneys fees for prevailing victims. The attorney general's office also would have been granted a cause of action.

Four additional bills were introduced in the House⁶ and one in the Senate that attempted to implement a breach notification requirement to protect residents of the commonwealth. Each bill would require the owner of the breached system to notify Virginia residents of the breach and makes an exception if notification may hamper a criminal investigation. Debate

among lawmakers appears to center around the following issues:

- **Civil rights**—Are victims of identity theft entitled to bring their own causes of action for damages? Treble damages?
- **Periodic credit reports for victims**—Should the company whose system was breached pay for consumers to receive periodic credit reports for a period of time following the breach? For how long?
- **Definition of “personal information”**—How much information do hackers need to steal a consumer’s identity? Last name and date of birth? Social Security number and mother’s maiden name?

The next logical question then becomes: Will lawmakers be able to keep up with the pace of hackers who acquire more and more information about an individual with less and less data; or will legislators continue to play catch-up?

Credit Freezes

If you have ever been a victim of identify theft, you have experienced the peculiar feeling of being assaulted without physical injury. A first step for victims to recover their identities, restore their credit and halt the progression of financial harm is to freeze access to their credit reports. Freezing access to credit reports prevents the identity thief from opening new lines of credit, securing loans and obtaining services in the victim’s name.

Five bills in the House⁷ and three in the Senate⁸ fell short of enactment as security- or credit-freeze legislation. Each draft attempted to establish guidelines for consumers and credit-reporting agencies, and each varied on timing of the service (from two to five business days to implement a freeze), fees for services (from \$5 to \$20 per freeze or lift), and damages (\$100, as provided under the Virginia Consumer Protection Act, up to \$1,000⁹). Some of the open issues include whether the credit agency is required to notify the consumer whose credit is frozen that an attempt has been made to access his or her credit and whether consumer notices of the right to a credit freeze must be issued.

The Future of Privacy Law— What’s Next?

In the wake of the Virginia Tech shootings of May 2007, Virginia legislators are likely to redirect at least a portion of their efforts away from protecting privacy and toward disclosure of private information—namely mental health records, for the protection of the public at large. In fact, Governor Timothy M. Kaine has already made strides in that direction by issuing an executive order requiring that any adjudication resulting in involuntary treatment for mental illness be reported to the national database related to the purchase of firearms.¹⁰

Still, it seems likely that we will see significant legislation passed at the federal level this year, in the area of data security-breach notification and credit freezes. As a result, companies that maintain databases of personally identifiable information or enter into contracts relating to management of data should be ready to take necessary steps toward compliance. Contracts for services involving data should commit the vendors (whether data-center providers, information technology consultants, application service providers, or others who will have the potential for involvement in a data security breach) to

comply with changing requirements (not just existing ones), to cooperate in remediation following any breach, and to share the costs of such compliance. ☪

Endnotes:

- 1 See *Griswold v. Connecticut*, 381 U.S. 479 (1965).
- 2 See <http://www.ftc.gov/opp/index.shtml>.
- 3 See Va. Code § 59.1-196 et seq.
- 4 See HB 2600, 2007 Gen. Assem., Reg. Sess. (Va. 2007)
- 5 See HB 1154, 2007 Gen. Assem., Reg. Sess. (Va. 2007)
- 6 See HB 995, 2007 Gen. Assem., Reg. Sess. (Va. 2007); HB 1508, 2007 Gen. Assem. Reg. Sess. (Va. 2007); HB 2140, 2007 Gen. Assem. Reg. Sess. (Va. 2007); HB 3148, 2007 Gen. Assem. Reg. Sess. (Va. 2007)
- 7 See HB 1877, 2007 Gen. Assem. Reg. Sess. (Va. 2007); HB 2681, 2007 Gen. Assem. Reg. Sess. (Va. 2007); HB 2804, 2007 Gen. Assem. Reg. Sess. (Va. 2007); HB 2963, 2007 Gen. Assem. Reg. Sess. (Va. 2007); HB 3056, 2007 Gen. Assem. Reg. Sess. (Va. 2007)
- 8 See SB 805, 2007 Gen. Assem. Reg. Sess. (Va. 2007); SB 946, 2007 Gen. Assem. Reg. Sess. (Va. 2007); SB 1030, 2007 Gen. Assem. Reg. Sess. (Va. 2007)
- 9 See SB 946.
- 10 See “Reporting Critical Safety Data to the Central Criminal Records Exchange,” Executive Order 50 (2007) Gov. Timothy M. Kaine; http://www.governor.virginia.gov/Initiatives/ExecutiveOrders/2007/EO_50.cfm



Melanie C. Holloway is an associate at McGuireWoods LLP in Richmond. She practices primarily in the areas of intellectual property, data and privacy law.



Janet P. Peyton is a partner at McGuireWoods LLP in Richmond. She leads the firm’s intellectual property, data and privacy practice group. She is the chair of the Virginia State Bar’s Intellectual Property Section.