Privacy and Data Security

Brian M. Gaff, Thomas J. Smedinghoff, and Socheth Sor
Edwards Wildman Palmer LLP

The third in a series of articles providing basic information on legal issues facing people and businesses that operate in computing-related markets focuses on the responsibility to ensure privacy and data security.

Recent years have seen an increasing number of well-publicized stories involving data security breaches and cybercrimes compromising all types of sensitive corporate and individual information. In addition to posing a serious threat to the businesses that are victimized, such incidents also present a significant risk of harm to the individuals and others affected by such breaches. In this month’s installment, we focus on the growing body of US and international law enacted to address these issues.

Be sure to check the IEEE Computer Society’s website for the podcast that accompanies this article (www.computer.org/portal/web/computingnow/computing-and-the-law).

OBLIGATIONS OF INFORMATION HOLDERS

The US and many other countries have enacted laws to address concerns regarding the privacy and security of both personal and corporate information. Those laws impose obligations on most businesses to protect the privacy of personal information, provide adequate security for corporate information, and disclose to those affected any breaches that involve personal information.

Data privacy

The focus of privacy law is on personal information. Generally, this includes any information relating to an identified or identifiable individual. It can be as little as a name, e-mail address, or phone number, or it can include much more extensive data such as an individual’s financial or health information.

Privacy laws regulate various aspects of the collection, use, processing, storage, and disclosure of all such personal information. US federal privacy law imposes comprehensive regulations in the financial and healthcare sectors, but there are few privacy rules outside those sectors. In the European Union and several other countries, however, all personal information is subject to comprehensive regulation in all sectors.

Most countries, including the US, often apply special rules to the privacy of more sensitive types of personal information, regardless of sector. In the US, depending on the jurisdiction, such rules might apply, for example, to Social Security numbers, drivers’ license numbers, information regarding medical or health conditions, credit or debit card numbers, and financial account information.

In the EU, data protection laws apply special rules to sensitive personal information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, or information specifying an individual’s sexual orientation.

Duty to provide security

A key aspect of most privacy laws is a requirement to protect the security of personal information. Even in the US, where many businesses aren’t directly subject to comprehensive privacy regulation, a variety of other laws impose a duty to provide security for personal information in all business sectors.
In most cases, there’s no single law, statute, or regulation that governs a company’s obligations to provide security for its information. Instead, there is an ever-expanding patchwork of statutes and regulations, common law obligations, contractual obligations, and industry standards. These combine to require companies to provide “reasonable” or “appropriate” physical, administrative, and technological security for their corporate data, especially personal information. For example, Massachusetts law requires any company—regardless of where it’s located—that maintains personal information about employees, customers, or other individuals who are Massachusetts residents to implement a comprehensive written information security program to protect such personal information.

Thus, a company’s duty to provide security can come from several different sources and several different jurisdictions—each perhaps regulating a different aspect of corporate information—but the result is a general obligation to provide security for all corporate data and information systems. In other words, information security is no longer just good business practice—it’s a legal requirement.

In addition, companies often assume additional security obligations voluntarily by contract. For example, outsourcing or similar agreements in which one business has access to the confidential data of its trading partner often require that appropriate security measures be taken to protect that data.

Similarly, businesses are often required to agree to security commitments as a condition of participating in certain activities. Thus, merchants that want to accept credit cards must agree to comply with the Payment Card Industry Data Security Standard (PCI-DSS).

**Legal standard for compliance**

Most of the laws and regulations that impose a duty to provide “reasonable” or “appropriate” security offer little guidance as to what specific security measures are required or how much security is enough. Instead, the law focuses on process, not on specific security controls. It requires companies to undertake a risk-based process to identify and implement measures that are reasonable under the circumstances to achieve the desired security objectives.

This means companies must assess the risks they face, identify and implement appropriate security measures in response to those risks, verify that they have effectively implemented those security measures, and ensure that they continually update those measures in response to new developments. Merely putting impressive-sounding security measures in place isn’t, by itself, sufficient.

For example, posting armed guards around a building or requiring key-card access might give the appearance of strong security, but if the primary threat the company faces is unauthorized remote access via the Internet, such physical security measures are of little value. Likewise, firewalls, intrusion-detection software, and encryption are often effective ways to stop hackers and protect sensitive databases. However, if a company’s major vulnerability is careless (or malicious) employees who inadvertently (or intentionally) disclose passwords or protected information, then even those sophisticated technical security measures, although important, won’t adequately address the problem.

As a result, the security measures necessary for legal compliance will vary depending on the situation, with the organization holding the data bearing the risk of making legally compliant decisions.

**Duty to disclose data breaches**

In addition to laws that impose a legal duty to implement security measures to protect data, numerous laws also impose an obligation to disclose security breaches to the people affected. Typically, these laws require prompt disclosure of a breach.

Most breach notification laws apply to personal information consisting of a person’s first name or initial and last name, plus at least one of the following: Social Security number, drivers’ license number, financial account number, credit card number, or debit card number. Some states add additional information to this list, such as medical information or biometric data.

By requiring notice to individuals who might be adversely affected by a security breach—for example, someone whose compromised personal information might be used to facilitate fraud or identity theft—these laws provide people with a warning that their personal information may or has been compromised. Those notified can then take steps to protect themselves against the consequences of fraud or identity theft. Keep in mind, however, that various regulatory enforcement agencies and state attorneys general are using these notifications to launch investigations into whether the business that suffered the breach met its legal obligations to provide appropriate data security.

In the US, 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted data breach notification laws—only Alabama, Kentucky, New Mexico, and South Dakota haven’t. Additional federal regulations exist in the financial and healthcare sectors. In Europe, several countries have enacted similar laws, and a January 2012 proposal for an EU-wide privacy regulation would...
extend such an obligation to all countries in the EU.

BE PREPARED

No level of security is perfect. Therefore, every business should develop an incident response plan so that it’s prepared in advance to deal with the consequences of security breaches that will inevitably occur.

Such a plan should ensure that appropriate individuals within the organization are promptly notified of any security breach, and that an appropriate team is assembled to respond. The plan should include procedures for evaluating, investigating, and containing security incidents. This involves protocols for working with law enforcement, forensics investigators, and other experts, and for communicating with government agencies, the press, and others who might be affected by a particular security breach.

Having a comprehensive security program in place to defend against data breaches, along with a plan to respond to the breaches that do occur, is critical to all companies operating in today’s digital business environment. This is particularly true in view of the frequency of breaches, many of which are widely publicized. Given the complexity of this issue and the myriad laws affecting it, it’s essential to consult a qualified attorney for advice on how to proceed.

Brian M. Gaff is a senior member of IEEE and a partner at the Edwards Wildman Palmer LLP law firm. Contact him at bgaff@edwardswildman.com.

Thomas J. Smedinghoff is a partner at Edwards Wildman Palmer. Contact him at tsmedinghoff@edwardswildman.com.

Socheth Sor is an associate at Edwards Wildman Palmer. Contact her at ssor@edwardswildman.com.

The content of this article is intended to provide accurate and authoritative information with regard to the subject matter covered. It is offered with the understanding that neither IEEE nor the IEEE Computer Society is engaged in rendering legal, accounting, or other professional services or advice. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.