A Publication of Law Bulletin Publishing Company
Chicago Lawyer®
Info Tech Law

Privacy and liability in a connected world

August 2008

BY ALAN S. WERNICK, ESQ., FSB FISHERBROYLES, LLP T: 847.786.1005 – E: WERNICK@FSBLEGAL.COM

Computing connectivity is usually equated with convenience. Plug in the USB memory device you carry in your pocket to the company network, download the business data, and off you (and the data) go. Quick. Easy. And potentially fraught with legal risks and liabilities for you, the business, and the customer or client.

There are a number of ways to get connected to data nowadays, including Universal Serial Bus (USB) devices, Bluetooth devices, Infrared (also called IR or IrDA [Infrared Data Association]) devices, Radio Frequency Identification (RFID) devices, WiFi (wireless fidelity), and hand-held hard drives that can hold many gigabytes of data.

Many of these devices are small enough to put on the end of a key chain or carry in a shirt pocket. Each of these devices can enable the user of the device to copy significant amounts of confidential personal data in less time than it took you to read this paragraph.

In the future, the myriad of electronic connectivity devices will be shrinking in size while increasing in storage capacity. Small, portable, high-capacity hard drives without any moving parts are already entering the marketplace. Consider the potential of a physician being able to carry a patient's entire medical history in the palm of the hand along with, and integrated with, medical and drug interaction reference texts. And consider the potential of patients being able to carry a card in their wallet that has their entire medical history from birth to present. Now, consider the potential liabilities for the loss of this valuable data or the inaccurate recording of this critical data.

Various state legislators and U.S. Congress have given considerable thought and analysis to these potential risks and liabilities for this valuable, critical data. The federal laws include some familiar names, such as the Health Insurance Portability and Accountability Act, Financial Services Modernization Act (otherwise known as Gramm-Leach-Bliley), and Sarbanes-Oxley Act.

The courts are weighing in on this subject as well. When actual harm, either economic or physical, results from identity theft, the courts have awarded damages.

Indeed, a number of states have passed data-breach legislation. Businesses may also experience liability for damages as a result of failing to act in accordance with all of the applicable data-breach laws. Which data-breach law applies may depend on the residence of each of the affected individuals in the compromised database, and not the location of the entity that experienced the data breach.

While financial damages to a business from a data breach can be significant, they can pale in comparison to a potentially far more deadlier damage — the loss of trust by those who entrusted you to protect their personal identifiable information. This loss of trust can potentially have a far greater negative impact on your business than any out-of-pocket financial damages award.

What can businesses do to manage the risks of liability for data breach as a result of interconnectivity? Steps for consideration include:

- Have a legal audit done by knowledgeable legal counsel (preferably one with a technology background and familiarity with data privacy, security, and compliance). A legal audit includes interviewing people in your organization, reviewing your practices and procedures (for instance, reviewing your vendor contracts for data privacy and related risks), and identifying the strengths and weaknesses of your compliance with the applicable statutes and laws, as well as identifying potential risks regarding data privacy and data security.
- Have a security audit done by a knowledgeable security professional working with knowledgeable legal counsel.
- Use encryption to secure the data at all times.
- Require users to use at least two security elements for interconnectivity access: (1) something they know—a strong password (that is changed periodically), and (2) something they must carry with them (in addition to the interconnectivity device), for example, a security token that generates a unique random number linked to the network's main server.
- Obtain appropriate insurance coverage for data breach losses.
- Educate users about data security and data quality.

Finding the balance between interconnectivity and risk management for data privacy, data security, and data quality will not be easy. Putting together a team from within your organization along with outside advisers is one proactive, preventive approach to finding that balance and managing the risks. While this approach may be expensive, it will be far less expensive than the increased lost management time, and increased legal expenses involved in having a court or government agency handle the problem for you.

Interconnectivity issues will only increase over time as new technologies allow for new ways to access data. While the legal risks can be managed, they may not be entirely removed. It is a process. As the old Chinese saying goes, "If you don't know where you are going, any road can take you there." Which road will you take to connect with your data?

