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

Computing connectivity risks

March 2013

BY ALAN S. WERNICK, ESQ.
T: 847.786.1005 – E: ALAN@WERNICK.COM

Computing connectivity is usually equated with convenience. However, this convenience can prove to be a liability for many organizations. Depending on how the business' computer hardware and systems are configured, any employee (or contractor or visitor) can plug a memory device into the network and download data, or upload the data to private cloud storage. This type of transaction is potentially fraught with legal risks and liabilities for the business.

There are a number of ways to get connected to data nowadays, including universal serial bus (USB) devices, Bluetooth devices, infrared devices (also known as IR or IrDA), radio frequency identification (RFID) devices, wireless fidelity (Wi-Fi) and handheld hard drives that can store gigabytes of data (e.g., your smartphone). Many of these devices are small enough to put on a key chain or carry in a pocket. Each lets the user copy significant amounts of confidential personal data in less time than it took you to read this paragraph.

In the future, the myriad electronic connectivity devices will shrink in size while increasing in storage capacity. Small, portable, high-capacity hard drives are already commonplace in the consumer marketplace. Consider, for example, the potential opportunities and risks of physicians carrying a patient's entire medical history, integrated with various medical and drug interaction reference texts, in their hands. Consider the potential opportunities and risks for patients carrying electronic cards containing their entire medical history, from birth to the present day, in wallets.

Insurance companies, state legislators, Congress and the courts have given considerable thought and analysis to these potential opportunities, risks and liabilities. Indeed, Congress and many states have passed privacy and-or data breach legislation. These laws include familiar names such as Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley and Sarbanes-Oxley.

Over the past few years, data thefts or misappropriations have been reported in the news, including data losses involving USB devices and CD-ROMs. In one case, an accountant had a CD-ROM containing confidential client information stolen from her car including the names, birth dates and Social Security numbers of about 30,000 participants and beneficiaries of pension and annuity funds. The clients sued the accountant for $200,000 in credit monitoring and insurance expenses incurred to mitigate the losses for potential misuse of the stolen client information. The accountant made a claim under her homeowner's policy and the insurance company refused to pay. The U.S. Court of Appeals, 7th Circuit, recently held that the policy did not cover the data loss. "Because the handling and care of confidential information is vital to [her] work as an accountant, the compact disk containing such information is a necessary, rather than incidental, element of her ordinary employment activities." The court held that the "business" exclusion from the policy applied. *Nationwide Ins. Co. v. Central Laborers' Pension Fund.*

As identity theft and data breach cases evolve, plaintiffs with actual economic damages as a direct result of identity theft resulting from a data breach most likely will present this legal basis for standing as a foundation to determine their damage and the defendant's liability. An individual's damages for identity theft may include (by way of example and not limitation) financial losses from the victim's bank account, renewal fees for lost identification cards (such as a driver's license), loss of medical benefits, identity theft remediation costs and attorney fees. Damages will depend on the actual facts of each case. Businesses, not-for-profit organizations and governmental units may also experience liability as a result of failing to act in accordance with applicable data breach and-or privacy 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 had the breach.

While financial damages to a business from a data breach can be significant, they can pale in comparison to a potentially far more deadly damage to an organization — the loss of trust from customers who entrusted the organization to protect their information. This loss of trust can potentially have a far greater negative impact on the institution than any out-of-pocket financial damages award. For example, such loss could jeopardize a hospital's electronic health records implementation or its programs for improvement of quality care.

Finding balance between interconnectivity and risk management for data privacy, data security and data quality will not be easy. Putting together a team of people from the organization and outside advisers is one proactive preventive approach. Of course, some organizations take the approach of waiting until a problem occurs. While the first approach is 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.

Interconnectivity issues will only increase over time. As the proverb 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?