The Continuing Battle Over Privacy vs. Security

by ELLEN C. CORNELIUS

Wed, October 14, 2015

In this electronic age, there is a constant struggle between sharing critical information and protecting individual privacy with adequate security to prevent data and documents from falling into the wrong hands. To address these concerns, expectations of privacy, knowledge of liabilities, and development of policies must be examined.

Some people might argue that there is virtually no privacy left as the Internet, government, and media dramatically affect daily routines. Others would say that, although daily life is not as private as it once was, privacy is a worthy sacrifice in order to defend against hackers and terrorists. The battle for a clear winner continues to rage, while several questions remain:

- How do expectations of privacy change based on security concerns?
- Who is liable in the aftermath of data breaches and identity theft?
- Are there policy solutions that could help balance these concerns?

"About 75 percent of health records are electronic, and healthcare providers use mobile devices to store, process, and transmit patient information. If a mobile device is hacked, then the healthcare provider or business associate may face penalties."

Expectations of Privacy

The expectation of privacy is deeply rooted in legal tradition and culture. For example, published in 1890, "The Right to Privacy," was a seminal article by Samuel Warren and Louis Brandeis (later a Supreme Court Justice) that still resonates today. Against the backdrop of the invention of the camera and the coverage of upper class society in the gossip pages of local newspapers, Warren and Brandeis' article in the *Harvard Law Review* explained the right of the individual citizen to be left alone. They started first with principles. The U.S. Constitution provides the right to life, liberty, and property. Property law protects the tangible, such as land and personal possessions, as well as the intangible, such as trade secrets and trademarks. Warren and Brandeis asserted that the right to privacy emerges from the right to life and liberty.

The right to privacy does not prohibit publication of material that is in the public or general interest. However, common law – or norms embodied in judicial decisions – protects an individual from being compelled to express his or her thoughts, sentiments, or emotions, except on the witness stand. The individual retains the power to limit publicity but, as soon as the individual decides to publish information, the right to privacy with respect to that particular piece of information is waived. If a person limits publicity, but a reporter uses a camera to take pictures surreptitiously, then the only applicable law is torts or, in this case, a lawsuit claiming invasion of privacy. Warren and Brandeis argued that the courts should protect the right to be left alone – that is, one's right to privacy.

Expectations of privacy change depending on security concerns. For example, closed-circuit television (CCTV) has attracted attention from privacy advocates who argue that they should be able to travel discreetly, without the government's knowledge. With CCTV, facial recognition software, and international databases, a person can be tracked on every continent around the world. Abuses by law enforcement and computer errors can be difficult to identify and correct. However, many of these fears have been addressed by cities in laws that regulate or limit how visual footage may be used by the government.

MORE IN CYBER & IT

The Continuing Battle Over Privacy vs. Security
How to Deploy an Ethical Cybercommunications Program
InfraGard - Over 400 Sector Chiefs in 84 Chapters
How to Make a 'Smart' Phone 'Undumb' in a Disaster
Cybersecurity as an Emergency Management Function
Solar Storm Near Miss & Threats to Lifeline Infrastructure
Cyber Grand Strategies: Technology vs. Human Interaction
Security Technology Trends to Watch in 2014
Insider Threats: A Call for Greater Vigilance
Holistic Security - Various Ways to Reduce Vulnerability

Beyond government interests, the general public takes photos and videos constantly. In a sense, individuals surveil each other. Facebook has perhaps the largest facial recognition database in the world. National level and local level law enforcement are heavily invested in facial recognition databases and software as well. In 2005, the identities of terrorists in London were discovered in a few weeks after they attacked three underground stations and a double-decker bus. In 2013, the terrorists who attacked the Boston Marathon were identified within a few days. Boston, Massachusetts, had only 55 law enforcement cameras in 2007 and the number has grown. Facial recognition software has made searching footage much faster.

Security advocates might say that observing possible terrorists and criminals makes communities more secure. They support increasing the number of cameras and license plate readers and argue that cameras with features like high definition, the ability to zoom in, and automated movement to focus on gunshots provide law enforcement with important opportunities to prevent and solve crimes. In response, policies to mitigate the impact of this technology focus on who can view the footage, how it can be used, and how long the recording will be kept.

Breaches, Thefts & Liabilities

Data breach, identity theft, and corporate liability are of great concern. In June 2014, over 1 million CareFirst BlueCross BlueShield subscribers had their personal data stolen. The first class-action lawsuit alleges negligence, breach of contract, and violations of Washington, D.C.'s consumer protection and data-breach notification statutes.

The Anthem breach announced in February 2015 was even bigger. Payment data was transmitted through the BlueCard network, but the data was being retained in an unencrypted fashion. It involved 80 million subscribers and has spawned more than 50 class-action lawsuits. Claims include violations of the Health Insurance Portability and Accountability Act (HIPAA) and state laws. However, data breach and identity theft are not just risks for insurance companies or healthcare systems. Many employers, big or small, maintain employees' names, addresses, social security numbers for tax purposes, and bank account information for payroll. There are at least three different ways that businesses can be liable for data breaches: HIPAA regulatory liability; negligence; and state statutory liability.

Medical identity theft can be used to falsify medical history, get surgeries, obtain or sell prescription drugs, and blackmail. Electronic medical records can be sold illegally for about $50 each, whereas cyber thieves may only earn $1 for social security numbers. Under HIPAA, any organization that handles patient information under a "business associates agreement" with a HIPAA-covered entity is equally liable for breaches as the covered entity itself, in accordance with the law. The courts often rely on HIPAA's privacy and security rules as the standard of care in negligence cases. Other best practices that the courts rely on include: encryption, monitoring of business associates, mitigation of risks, and increased accountability.

The U.S. Department of Health and Human Services (HHS) recommends administrative, physical, and technical safeguards to protect patient information:

- *Administrative safeguards* include security management processes, security personnel, information access management, training and management, and evaluation.
- *Physical safeguards* include facility access and control as well as workstation and device security. A HIPAA-covered entity must: limit physical access to its facilities while ensuring that authorized access is allowed; implement policies and procedures to specify proper use of and access to workstations and electronic media; and have policies and procedures regarding the transfer, removal, disposal, and reuse of electronic media to ensure appropriate protection of electronic protected health information.
- *Technical safeguards* include access control, audit control, integrity control, and transmission security.

Businesses may be liable for civil penalties if the courts determine that they are negligent in protecting electronic health records. According to the U.S. Department of Health and Human Services, about 75 percent of health records are electronic, and healthcare providers use mobile devices to store, process, and transmit patient information. If a mobile device is hacked, then the healthcare provider or business associate may face penalties. In July 2015, the National Institute of Standards and Technology, National Cybersecurity Center of Excellence, issued a "How to Guide," which provides a sample solution for protecting electronic health records on mobile devices. The guide uses commercially available products to more securely share electronic health records. A court may use this as the standard of care and apply it in

negligence cases.

Four elements are required to establish a case of negligence: duty, breach, causation, and damages. Reasonable care speaks to duty. Principal factors to consider in ascertaining whether the person's conduct lacks reasonable care include: (a) the foreseeable likelihood that this conduct will result in harm; (b) the foreseeable severity of any harm that may ensue; and (c) the burden of precautions to eliminate or reduce the risk of harm (see Restatement [Third] of Torts: Liability for Physical Harm § 3 [P.F.D. No. 1, 2005]). Negligent conduct may consist of either an act, or an omission to act when there is a duty to do so (see Restatement [Second] of Torts § 282 [1965]).

Businesses have a duty to safeguard customer information. For example, Maryland's Social Security Number Privacy Act requires employers to transmit social security numbers over the Internet with a secure connection or encryption. Businesses should know what personal information the organization has on its computers, then secure that information physically, with passwords, or with assigned identification numbers that are different from the social security numbers.

Many companies spend a significant amount of money on antivirus products and firewalls, but hackers can breach such perimeters. What companies really need are detection products that stop an attack once the system has been breached. Hiring and training also are important. Organizations should train employees on the data security plan, as well as on protocols so employees can spot, report, and remedy potential security threats. Background checks on employees who have access to personally identifiable information are also important, while confidentiality agreements can be used to address security with contractors.

Liability can also ensue from a violation of a state statute. For example, the Maryland Personal Information Protection Act requires an employer to maintain reasonable security procedures and practices for personal information. Consumers must receive notice of a data breach, and the notice must include:

- A description of the information compromised;
- Contact information for the business, including a toll-free number if the business has one;
- Toll-free numbers and addresses for Equifax, Experian, and TransUnion;
- Toll-free numbers, addresses, and websites for the Federal Trade Commission and the Office of the Attorney General of Maryland; and
- A statement that the individual can obtain information from these sources regarding steps to avoid identity theft.

Policy Solutions to Address Concerns

There are also policy developments in cybersecurity to consider. For example, in the healthcare industry, the development of a unique patient identifier is under consideration. Currently, medical record numbers are not unique and not transferable. Another policy proposal is that businesses create business continuity plans, so they can continue to operate if the organization's data were catastrophically breached.

The federal Cybersecurity Information Sharing Act of 2015 (S.754) has been proposed to promote the sharing of cyberthreat information among government agencies and private sector businesses. As drafted, S.754 would offer incentives to the private sector to share information about cyberthreats with the government. Supporters, including senators from both parties and many in the private sector, say the information sharing legislation would create stronger defenses against hackers. However, privacy advocates are concerned about the bill's treatment of sensitive information, arguing that it would violate the right to privacy. Moreover, security experts have questioned whether the bill would be effective.

Against this complicated backdrop, policy makers continue to try to balance privacy and security. Privacy advocates push back against the use of technology to monitor threats and favor tighter regulations, whereas security advocates push for a more widespread use of technology and the development of threat-detection tools. Undoubtedly, there are many challenging calls to be made in the year ahead.

Ellen C. Cornelius, J.D., is senior law and policy analyst at the University of Maryland Center for Health and Homeland Security (CHHS) and an adjunct professor at the University of Maryland Francis King Carey School of Law, where she teaches a course entitled Law and Policy of Cybersecurity. Her article, "Chinese Hackers and their New Target – Federal Employees," was published in the 2014. Through CHHS, she has been detailed to the District of Columbia (D.C.) Homeland

Security and Emergency Management Agency since 2008. She has drafted a variety of plans for D.C., including the Emergency Shelter Plan. In 2013, she became the liaison to D.C.'s public-private institution – the Business Emergency Management Operations Center.