ES&A
A LAW CORPORATION

MEMORANDUM

To: ES&A Clients and Friends
From: Samantha M.P. Sneed
Date: 5/19/2016
Subject: Watching the Watches Watching Us: Developments in Privacy and Security

Computing costs have dropped like a rock. Devices have not only become smaller and more powerful, but there's likely one within arm's reach.[1] Devices and the services they enable have also become so integrated into our personal and professional lives that it's hard to find any space that isn't connected. This can create a host of privacy and security issues that you may not have been aware of.

I. The US Approach to Privacy

The U.S. is in the midst of an ongoing discussion on how individual privacy should be protected and what role private industry plays in that protection. We consider privacy to be a "penumbral right of the Constitution," meaning it is implied by the explicitly enumerated rights.[2] General principles in personal injury law offer basic protections of the right to privacy by making actions that could be considered "highly offensive to a reasonable person" a cause for a lawsuit.[3]

More stringent protections have been instituted piecemeal to protect certain industries or categories of individuals. We have broad protections for healthcare information, banking and credit information, and information about children.[4] Anti-discrimination laws and a number of marketing and telecommunications laws provide more targeted privacy protections for certain employees and consumers.[5] Unfortunately, information and persons not covered by existing laws or contracts are essentially fair game.

Laws mandating *mechanisms* to protect private information are similarly fragmented. Some privacy laws have been updated to incorporate information security (i.e., "cybersecurity") provisions.[6] However, a

[1] See "Technology Device Ownership: 2015," Pew Research Center (Oct. 29, 2015) available at http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/. The study estimates 92% of all adults in the United States own a cellphone, 73% own a desktop or laptop, and 45% own a tablet.

[2] See *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[3] See the Restatement (Second) of Torts.

[4] See the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Genetic Information Nondiscrimination Act (GINA), Health Information Technology for Economic and Clinical Health Act (HITECH), Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act, Fair and Accurate Credit Transactions Act, Dodd-Frank Act, the Bank Secrecy Act, Family Educational Rights and Privacy Act of 1974, Children's Online Privacy Protection Act of 1998.

[5] See the Civil Rights Act of 1964, the Pregnancy Discrimination Act, the Age Discrimination Act, Americans with Disabilities Act and Amendments, Equal Pay Act, Family and Medical Leave Act (FMLA), Employee Polygraph Protection Act of 1988, Electronic Communications Privacy Act, Whistleblower Protection Act, National Labor Relations Act, Cable Television Privacy Act of 1984, the Video Privacy Act of 1988, Telephone Consumer Protection Act, Telemarketing and Consumer Fraud and Abuse Prevention Act, Telecommunications Act of 1996, and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM).

[6] See, for example, the HIPAA Privacy Rule, enacted in 2000 and revised in 2002, the HIPAA Security Rule, enacted in 2003.

number of recent federal initiatives, highly-publicized legal battles, and proposed legislation suggest that changes might be on the way:

- The NIST Cybersecurity Framework, released in 2014 and reviewed last month, is a voluntary framework that applies multiple industry standards to allow organizations to assess risk to their electronic and physical assets, establish precautionary measures, and respond to threats and breaches.
- In reaction to the 2015 Office of Personnel Management breaches, the Department of Defense (DoD) issued changes to the Defense Federal Acquisitions Regulations that greatly increases the security and reporting obligations for defense contractors.[7]
- The Apple-FBI debate on encryption earlier this year highlighted the tension between individual privacy rights, advanced technological means to secure private information, and the government's interest in compelling private industry to defeat their own systems.
- The Compliance with Court Orders Act of 2016, proposed in response to the Apple-FBI standoff, would require "any person who provides a product or method to facilitate a communication or the processing or storage of data" to provide "intelligible" (i.e., decrypted) data to a government agent upon issuance of a court order.

II. Possible Guidance From US Trade Partners

It is possible that in revisiting our laws on privacy and security U.S. lawmakers will look to more comprehensive systems implemented by our trade partners. For example, the European Union explicitly recognizes a right to personal privacy and the protection of personal data as a natural right.[8] Private organizations are obligated to provide basic protections for "personally identifying information" stored in a database.[9] The EU even goes so far as to recognize the "right to be forgotten" and "right of erasure," which obligates ALL parties who hold individuals' personal information to honor the requests of individuals to remove the information from their databases.

Asia as a region takes a more trade-oriented approach to most regional privacy and security agreements and frameworks. For example, the 2005 APEC Privacy Framework, established to develop online business in the Asia-Pacific region, assigns responsibility for the protection of personal information to all entities that receive such data. Similarly, the Trans Pacific Partnership (TPP) includes a number of provisions designed to regulate information transfers throughout the region to protect personal information and intellectual property.

---

7 For a good summary of the changes, see "A Guide to Complying with DoD's New Cybersecurity Rules," Law 360, (Sept. 21, 2015) available at http://www.law360.com/articles/705295/a-guide-to-complying-with-dod-s-new-cybersecurity-rules.

8 Charter of Fundamental Rights of the European Union, 364/1, art. 8, 2000 O.J. (EC).

9 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, art. 2(a) 1995 O.J. (L 281) (EC).

III. Why Changes to Privacy and Security Policy Is Important For Organizations Not Named Apple and Google

The U.S. has already taken steps toward comprehensive protection of personal data with the APEC Privacy Framework, TPP, and measures such as the White House's proposed Consumer Privacy Bill of Rights Act. It's not yet clear what the ultimate scope of those protections will be, what mechanisms will be used to secure them, and who will be tasked with compliance. However, it's very likely that employers and private industry will be made to play a major role in ensuring the privacy and security of its customers *and* employees.

Mobile networked devices can store sensitive information and easily travel, meaning there is always a risk that sensitive personal and business information may virtually or literally walk out your doors. However, in a post-*Purple Communications* world, it has become more difficult for employers to exert control over the communications within their organizations. The situation is made even more complicated in workplaces that allow their employees to take laptops and other devices home or bring in their own ("BYOD").

Allowing technology to do double duty in our professional and personal worlds means that a problem on one side will likely find its way to the other. It also means that protecting your organization's resources (or protecting your organization from its resources) will require an active and ongoing collaboration between management, IT, HR, and legal. It is unlikely that we will stop using smart phones, tablets, or that nice Bluetooth-connected coffeepot you found on Amazon any time soon. However, as devices become more omnipresent and comprehensive, so must the law, and so must an organization's approach to navigating it all.