GEORGE MASON AMERICAN INN OF COURT

WHAT YOU NEED TO KNOW ABOUT CYBERSECURITY

November 28, 2017

Team Members:

Honorable John M. Tran
Jay V. Prabhu, Esq.
Steve Britt, Esq.
Ryen Rasmus, Esq. (Team Leader)
Louise T. Gitcheva, Esq.

Philip Abbruscato (Student Member)
Kyle Armstrong (Student Member)
Danny Alvarado (Student Member)

I. Regulatory Framework – United States Cyber security laws
   a. 2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA): Applies to every government agency, "requires the development and implementation of mandatory policies, principles, standards, and guidelines on information security" to ensure the security of data in the federal government.
      i. The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner.
   b. Cybersecurity Information Sharing Act (CISA): Authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats.
      i. CISA provides certain protections to encourage companies voluntarily to share information—specifically, information about "cyber threat indicators" and "defensive measures"—with the federal government, state and local governments, and other companies and private entities.
      ii. These protections include protections from liability, non-waiver of privilege, and protections from FOIA disclosure, although, importantly, some of these protections apply only when sharing with certain entities.
   c. Cybersecurity Act of 2015: Establishes a voluntary framework for confidential, two-way sharing of cyber threat information between private sector and U.S. government, via a Department of Homeland Security portal; offers protection from liability for sharing.
   d. Computer Fraud and Abuse Act: Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication shall be punished under the Act.
   e. Foreign Intelligence Service Act (FISA): Designed primarily for intelligence gathering agencies to regulate how they gain general intelligence about foreign powers and agents of foreign powers within the borders of the United States.
   f. Electronic Communications Privacy Act (ECPA): Handle electronic surveillance, interceptions, and access to data, for domestic law enforcement purposes for criminal investigations involving people in the United States
   g. PATRIOT Act: Allows federal officials greater authority in tracking and intercepting communications, both for purposes of law enforcement and foreign intelligence gathering.
   h. Wiretap Act: Regulates the interception of a communication through the use of any electronic, mechanical or other device. Applies when communications are intercepted contemporaneously with their

transmission. Once the communication is completed and stored, the Wiretap Act no longer applies.

i. To allow a wiretap, a judge must find probable cause and that the particular communication concerning the offense will be obtained through the interception.
    1. Alternatives to wiretapping must have been attempted and failed, or reasonably appear to be unlikely to succeed or to be too dangerous.
    2. The order can last for up to 30 days and can be renewed.

II. State laws: Fills in the gap of federal law, but can set *de facto* national standards
   a. Virginia:
      i. Virginia Personal Information Data Privacy Notification And Encryption Laws: Va. Code § 18.2-186.6
         1. Unlike similar state laws, this includes a provision for imposing financial penalties for noncompliance
      ii. Virginia Compute Crimes Law
         1. Covers the intentional trespassing into computer network, use of a computer for fraud, and various other crimes involving a computer are prohibited under state laws.
         2. In Virginia, computer crimes also include invasion of privacy and computer harassment. The state separates offenses into misdemeanors and felonies, with the more serious crimes involving theft. Attempt is not considered a crime, but Virginia does allow civil lawsuits for damages related to computer crimes.

III. Key Industries with Cyber Security Regulations
   a. *Healthcare:* Controlled under the 1996 Health Insurance Portability and Accountability Act (HIPAA).
      i. Regulates medical information. It can apply broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information. The Standards for Privacy of Individually Identifiable Health Information apply to the collection and use of protected health information. The Security Standards for the Protection of Electronic Protected Health Information provides standards for protecting medical data. The Standards for Electronic Transactions applies to the electronic transmission of medical data. These HIPAA rules were revised in early 2013 under the HIPAA "Omnibus Rule".
      ii. The HIPAA Omnibus Rule also revised the Security Breach Notification Rule which requires covered entities to provide notice of a breach of protected health information. Under the revised rule, a covered entity must provide notice of acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, unless the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised.

b. *Insurance and Financial Services*: Must comply with the Gramm-Leach-Bliley Act which requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
c. *Telecommunications Carriers*: Current communication cybersecurity issues involve the management and transfer of customer databases, the appropriate uses of position-location technology, and special statutes such as the Cable Television Consumer Protection and Competition Act governing cable subscriber information or, under the Communications Assistance for Law Enforcement Act (CALEA) establishing technical facilities cooperation responsibilities.
    i. CALEA requires a "telecommunications carrier," to ensure that equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization.
    ii. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment design and modify their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve.
    iii. CALEA is limited to Telecommunications Carriers as defined by the Act and interpreted by the FCC. In addition, CALEA specifically exempts "Information Services", which includes many Internet based communications service providers, electronic storage providers and electronic messaging services.
d. *Government Contracts*: Federal contractors are increasingly targeted by cyber attacks due to the sensitive nature of government information that is generated, received and stored on their systems. In response to these attacks, as well as high-profile attacks on government-owned information systems and insider threats, the government has adopted stringent information security protocols and cyber incident reporting obligations.
    i. On May 16, 2016, the Federal Acquisition Regulation (FAR) was amended to implement requirements for the "Basic Safeguarding of Covered Contractor Information Systems" to apply to all government contractors. The intent is to establish basic safeguarding measures that are (or should be) generally employed by contractors as part of "routine" business practices – the rule is a baseline and does not impact other more specific federal information safeguarding requirements.

IV. Model Rules of Professional Conduct – Cybersecurity and an attorney's duty to safeguard confidential data of clients

a. Rule 1.1 Competence a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology...*"
    i. "A lawyer shall provide competent representation to a client." This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." It includes competence in selecting and using technology. It requires attorneys who lack the necessary technical competence for security to consult with qualified people who have the requisite expertise.
b. Rule 1.6 Confidentiality of Information: "(c) A lawyer shall make *reasonable efforts* to prevent the unintended disclosure of, or unauthorized access to, information relating to the representation of a client."
    i. Aug. 2012 addition to Comment [18]
        1. "reasonable efforts" considers, the sensitivity of the information. the likelihood of disclosure if additional safeguards are not employed and safeguards (cost, difficulty of implementing, and extent to which they adversely affect the lawyer's ability to represent clients)
c. Rule 1.4 Communication: Requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished," including the use of technology. It requires keeping the client informed and, depending on the circumstances, may require obtaining "informed consent." It requires notice to a client of a compromise of confidential information relating to the client.

V. <u>ABA Cybersecurity Resolution, Aug. 2014</u>
a. "RESOLVED, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an **appropriate cyber security program** that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected."

I. <u>What are the Various Kinds of Cyber Threats?</u>
a. Law firms are considered to be particularly vulnerable to cyberattacks.
    i. The extent to which law firms are subject to cyberattacks is unknown, as is the scope of cyberattacks against law firms.
    ii. As the cybersecurity knowledge of lawyers grows, it is unclear whether or not they are acting on it to protect clients' information from unauthorized access.
    iii. There is little incentive for lawyers to take reasonable cybersecurity action, because there is insufficient regulation and little to no meaningful consequences for inaction.
b. Lawyers are the targets of cyberattacks for three related reasons: "they store valuable confidential client information, they are likely to be more vulnerable than their clients, and they are under increased pressure to take advantage of technologies that render them susceptible to attacks."

c. Malicious insiders, or "disgruntled current and former lawyers and staff members," present a cyber threat.
d. Social engineers, state-sponsored hackers, corporate espionage, and financial criminals present a cyber threat.
e. The government also seeks to intrude and surveil.
    i. This cyber threat is of particular concern to criminal defense, immigration, and intellectual property lawyers who typically find themselves in an adversarial relationship with the government.
f. "96% of hacking attacks employ simple techniques, and 97% of attacks can be blocked by common security practices that are within the reach of even small law firms and solo practitioners."
g. "Malware is malicious software . . . 'encompasses a wide range of program types including viruses, worms, logic bombs, Trojan horses, keyloggers, zombie programs, and backdoors.'"
    i. Spray and pray is the tactic of sending out massive quantities of malware-infected emails in hopes of hitting as many individual targets as quickly as possible.
    ii. Some tailor messages to appear as genuine as possible, through social engineering to gain knowledge of a company's operating structure, invoice and remittance practices, and even individual's writing styles
    iii. A virus or worm is a piece of code capable of replicating itself with typically detrimental effect, ex. corruption of the system, destruction of files.
    iv. Logic Bombs are sets of instructions that have been secretly incorporated into a program so that once a particular condition is satisfied the effect of the instruction is activated.
    v. A Trojan Horse, similar to the ruse used to gain access to Troy, is a program which ostensibly performs an innocuous function, but, in reality, is designed to breach the security of a computer system.
    vi. Keyloggers are software or hardware that covertly captures keys struck on a keyboard to gain the victim's login information and passwords.
    vii. Zombie programs allow a wrongdoer to remotely access an infected computer to potentially perform malicious tasks.
    viii. Backdoors are ways to access a computer system or encrypted data. These can be preexisting or installed by the wrongdoer.
    ix. Scareware is "malware that 'takes advantage of people's fear of revealing their private information, losing their critical data, or facing irreversible hardware damage.'"
    x. "Ransomware is malicious software that encrypts data on a device or a system, then bars access to, or recover of, that data until the owner has paid a ransom."

1. “A category of malicious software which, when run, disables the functionality of a computer in some way”
2. Essentially the digital version of hostage taking.
3. “This type of threat has existed in some shape or form since at least 1989, but over the past two years the frequency and scope of attacks have increased to alarming levels.
4. “In the wake of the economic recession, Ransomware came back with a vengeance, making a dramatic entrance as it ‘resurged in 2013;’ it has continued to flourish ever since.”
    a. Resurgence can be partially explained by success of other hacking efforts.
5. Self-propagating features make it incredibly difficult to eliminate
6. Traditional breaches typically entail acquisition of data, Ransomware allows wrongdoer to control, damage, and interrupt systems; deny access to data; and destroy or otherwise harm data’s integrity—all without actual acquisition of data
7. Ransomware is frequently delivered through spear phishing emails to end user
    a. Mass phishing campaigns: malware installed on user’s computer without their knowledge when that user browses to a compromised website and is using outdated browsers, browser plugins, and other software
        i. Lawyers targeted by a phishing email with link to view a business complaint that opens a website that installs ransomware.
    b. The level of technological expertise required to engineer a Ransomware attack has decreased significantly, at this point deploying Ransomware is relatively low budget, low stakes, and doesn’t require much skill to pull off
8. Locker Ransomware: restricts user access to infected systems by locking up the interface or computing resources within the system thereby blocking off access to the compute or denying access to files
    a. Effectively changing the lock on the door, changing the mechanism by which the lock engages
    b. The victim is asked to pay to have the door unlocked.

9. Crypto Ransomware: encrypts files on the target system so that the computer is still usable, but users can't access their data
    a. Cracking the lock to avoid paying the ransom would take the average desktop computer 6.4 quadrillion years
    b. Sizes up each item within the unit, systematically determining relative value of files to user.
    c. While encrypting files, searches and steals Bitcoins from user
    d. Can threaten to release sensitive files unless ransom is paid.

xi. Ransomware appears poised to evolve along the same lines as many other noncriminal programming efforts, increasingly adopting the aesthetic and practicality of popular software instances that rely on a modular design, allowing criminals to use certain functions as-needed and offering much better efficiency and the ability to switch tactics as required in the event one method is discovered or is found to be ineffective.
    1. Trend seems to be toward attacks carried out on a more ambitious scale

h. Vendors are consistently cited as a primary cause of data breaches.
i. If lawyer is using cloud computing then the lawyer stores data on a computer owned by a third party.
    i. Because cloud computing places client data on remote servers not in a lawyer's direct control an issue is whether lawyers can use the cloud
    ii. Often using a cloud vendor is more secure than what a lawyer might be able to have on the lawyer's own computer systems
        1. Cloud vendor is likely to have better backup capability

II. <u>Why is Cyber Security Important for Our Clients?</u>

a. Technology is used extensively in the practice of law.
    i. Addition of phrase to Model Rule 1.1 Comment 8 by 2012 technology amendments stress that competent lawyers should be aware of basic features of technology
b. Compromised client information can lead to a loss "of the attorney-client privilege, fraud, negative publicity and tarnished business reputations, liability to others, and even bankruptcy."
    i. Loss of files may be eclipsed by the loss of client trust, relationships, and reputation

ii. Even if lawyer does not represent health care provider or financial institutions he or she is likely to have medical or financial information that raises the same or similar confidentiality issues
iii. One might argue that all confidential information, including attorney-client communications, should be protected with the same or similar safeguards.

c. Law firms and other organization—including vendors that provide preservation-related services—that have custody of these eDiscovery data sets should be cognizant of the risks created by atypical retention practices
    i. Data sets are no less susceptible to Ransomware than their standard counterparts—and may even be more attractive targets, given the one-off nature of eDiscovery collections as well as the highly sensitive data they contain
    ii. Ransomware may preserve data in a sense, but the data cannot be made available for production or may not exist in a usable format, which can add to the eDiscovery conundrums
d. Encryption complicates the user experience; encrypting all electronic information interferes with using the information efficiently.

I. Future of Cybersecurity – The growing threat involving the Internet of Things
a. The Internet of Things – can be defined as physical objects that connect to the internet through embedded systems and sensors, interacting with it to generate meaningful results and convenience to the end-user community
    i. The Internet of Things is the network of physical objects that contains embedded technologies to communicate and sense or interact with their internal states or the external environment
    ii. Enables the creation of an "environment" to provide services that can range from home automation to smart city services
    iii. Security issues that come with human usage of this "environment"
        1. Because human communication is mediated by machines and is more and more indirect, there is a deeply rooted security problem with the possibility of impersonation, identity theft, hacking and, in general, cyber threats
        2. Also, another security issue arises because of the need to use "cloud computing" for the intertwining of these "environments"
    iv. Industries that the Internet of Things will affect
        1. Healthcare – personal information and medical history of patients, sensors and microcomputers implanted in patients to monitor health, automated critical treatments for better efficiency
        2. Education - interactive smart classrooms to help students learn and participate more, automatic attendance and various student tracking systems (for school security), internet-enabled remote

classrooms will for developing countries without the infrastructure for schools

3. Manufacturing and Industrial - Plant and energy optimization, health and safety control and security management, through advanced sensors, and networked with sophisticated microcomputers

v. The Connected Car – one of the big possible security issues from The Internet of Things is the automated and connected car

1. Because the connected car "lives" in the network, security is not a matter of closing doors and encrypting data; security means managing shared data and a more complex network of participants.
2. The target of protection, the object of security, becomes the network of networks, not the individual car, and all cybersecurity measures and technologies need to be aligned with this goal in mind.
3. Security requirements must be addressed at the application/channel level, but in some cases, this blocks the ability of the auto manufacturer to have a coherent strategy
4. When considering connected car initiatives, businesses need to establish a solid legal understanding of data ownership and data protection policies.

II. <u>Challenges that Arise from Increase in Interconnectivity</u>

a. Traditional proven risk management models have their origins and wisdom still focused in a world where the organization owns and possesses most, if not all, of the data assets owing through the systems.
   i. The increasing use of the internet and mobile working means that the boundary of the enterprise is disappearing: and as a result, the risk landscape also becomes unbounded
b. Speed of Change – New product launches, mergers, acquisitions, market expansion, and introductions of new technology are all on the rise: these changes invariably have a complicating impact on the strength and breadth of an organization's cybersecurity, and its ability to keep pace
c. Cloud computing – Provides a platform for the Internet of Things to flourish but there are still many challenges when it comes to cloud security or data security in the cloud
d. Privacy and Data Protection – All smart devices hold information about their users, ranging from their diet plan to where they work; smart devices will include personal life details and often even banking details.
   i. All Internet of Things devices gather accurate data from the real world, but a user might not be comfortable with sharing that data with a third party — even if not all the data is confidential or sensitive.
   ii. Some of the top privacy risks also contain web application vulnerabilities, operator-side data leakage, insufficient data breach response, data sharing with third parties, and insecure data transfer

e. Growing Use of Mobile Devices – Smart phones contain our home address, credit card details, personal photos/videos, e-mail accounts, official documents, contact numbers and messages. The information stored on our devices will include the places that we visit frequently and a "pattern" that uniquely identifies us, so anyone who can hack into any of these devices can get into our lives very easily.
    i. The increase in the number of devices can also be a problem as the vulnerabilities that they are associated with will spread very rapidly. With thousands of vendors across the globe, it will be very difficult for the network engineers to patch these vulnerabilities, especially with thousands of new patches to update daily

III. <u>New Regulation to Strengthen Cybersecurity</u>

a. Internet of Things Cybersecurity Improvement Act of 2017 - would require that devices purchased by the U.S. government meet certain minimum-security requirements
    i. Vendors who supply the U.S. government with Internet of Things devices would have to ensure that their devices are patchable, do not include hard-coded passwords that can't be changed, and are free of known security vulnerabilities, among other basic requirements
    ii. Promotes security research by encouraging the adoption of coordinated vulnerability disclosure policies by federal contractors and providing legal protections to security researchers abiding by those policies.
    iii. Direct the Office of Management and Budget (OMB) to develop alternative network-level security requirements for devices with limited data processing and software functionality
    iv. Direct the Department of Homeland Security's National Protection and Programs Directorate to issue guidelines regarding cybersecurity coordinated vulnerability disclosure policies to be required by contractors providing connected devices to the U.S. Government
    v. Exempt cybersecurity researchers engaging in good-faith research from liability under the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act when in engaged in research pursuant to adopted coordinated vulnerability disclosure guidelines
b. Cybersecurity Information Sharing Act of 2015 –
    i. Requires the Director of National Intelligence and the Departments of Homeland Security (DHS), Defense, and Justice to develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threats.
    ii. The bill limits the purposes for which the government may use shared information to certain cybersecurity purposes and responses to imminent threats or serious threats to a minor. The crimes that may be prosecuted with such information are restricted to offenses relating to fraud and identity theft, espionage, censorship, trade secrets, or an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or use of a weapon of mass destruction.

iii. The Department of State must develop a diplomacy strategy to obtain agreements on international behavior in cyberspace and consult with countries regarding the prosecution and prevention of cyber or intellectual property crimes.
iv. The bill also allows criminal penalties for fraud involving account access devices to be imposed regardless of whether the underlying articles, property, or proceeds are held within, or have transferred through, U.S. jurisdiction.

c. Modernizing Government Technology Act of 2017 – authorizes each of specified agencies for which there are Chief Financial Officers to establish an information technology system modernization and working capital fund to:
i. Improve, retire, or replace existing information technology systems to enhance cybersecurity and to improve efficiency and effectiveness;
ii. Transition legacy information technology systems to cloud computing and other innovative platforms and technologies;
iii. Assist and support efforts to provide adequate, risk-based, and cost-effective information technology capabilities that address evolving threats to information security; and
iv. Reimburse amounts transferred to the agency from the Technology Modernization Fund (established under this bill), with the approval of such agency's Chief Information Officer.

IV. National Institute of Standards and Technology – *Framework for Improving Infrastructure Cybersecurity*

a. The United States Chamber of Commerce has urged the administration and foreign administrations to support this framework.
i. The White House and agency chiefs need to work with regulated industry sectors to harmonize cyber regulations with the Framework. The Chamber wants to see this initiative begin this year. Streamlining overlapping and/or conflicting cyber red tape is a top priority.
ii. The federal government should support ambitious public- and private-sector efforts to help private enterprises manage cyber supply chain risks internally and with their suppliers and partners.
iii. Government and business leaders should consider ways to help SMBs and state and local governments use the Framework and analogous tools.

User Name: Kyle Armstrong

Date and Time: Tuesday, October 17, 2017 4:34:00 PM EDT

Job Number: 55124754

Document (1)

1. *ARTICLE: RANSOMWARE -- PRACTICAL AND LEGAL CONSIDERATIONS FOR CONFRONTING THE NEW ECONOMIC ENGINE OF THE DARK WEB*

   Client/Matter: -None-

   Search Terms: ARTICLE: RANSOMWARE -- PRACTICAL AND LEGAL CONSIDERATIONS FOR CONFRONTING THE NEW ECONOMIC ENGINE OF THE DARK WEB

   Search Type: Natural Language

ARTICLE: RANSOMWARE -- PRACTICAL AND LEGAL CONSIDERATIONS FOR CONFRONTING THE NEW ECONOMIC ENGINE OF THE DARK WEB

Spring, 2017

Reporter
23 Rich. J.L. & Tech. 1

Length: 10472 words

Author: By: James A. Sherer, * Melinda L. McLellan, ** Emily R. Fedeles, *** and Nichole L. Sterling ****

* James A. Sherer is a Partner in the New York office of Baker & Hostetler LLP.

** Melinda L. McLellan is a Partner in the New York office of Baker & Hostetler LLP.

*** Emily R. Fedeles is an Associate in the New York office of Baker & Hostetler LLP.

**** Nichole L. Sterling is an Associate in the New York office of Baker & Hostetler LLP.

Highlight

James A. Sherer, Melinda L. McLellan, Emily R. Fedeles, and Nichole L. Sterling, *Ransomware -- Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, http://jolt.richmond.edu/2017/04/30/volume23_annualsurvey_sherer/.

Text

I. INTRODUCTION

P1 Ransomware is malicious software that encrypts data on a device or a system, then bars access to, or recovery of, that data until the owner has paid a ransom. [1] This type of threat has existed in some shape or form since at least 1989, [2] but over the past two years the frequency and scope of attacks have increased to alarming levels. In response, the U.S. Federal Trade Commission (FTC) identified Ransomware as "one of the most serious online threats facing people and businesses" in 2016 as well as "the most profitable form of malware criminals use," [3] and the FBI developed a special working group dedicated to fighting it. [4]

---

[1] *See* Krzysztof Cabaj & Wojciech Mazurczyk, *Using Software-Defined Networking for Ransomware Mitigation: the Case of CryptoWall*, 30 IEEE NETWORK 14 (2016).

[2] *See* JAMES SCOTT & DREW SPANIEL, THE ICIT RANSOMWARE REPORT: 2016 WILL BE THE YEAR RANSOMWARE HOLDS AMERICA HOSTAGE 3-4 (2016).

[3] Ben Rossen, *How to Defend Against Ransomware*, FTC (Nov. 10, 2016), https://www.consumer.ftc.gov/blog/how-defend-against-ransomware, https://perma.cc/CJA5-BV2B.

[4] *See* Paul Merrion, FBI Creates Task Force to Fight Ransomware Threat, CQ ROLL CALL, Apr. 4, 2016, 2016 WL 2758516.

P2 Considering that Ransomware emerged "at the dawn of the Internet revolution," [5] even before the development of formalized Internet law and policy, attorneys have now had a bit of time to become familiar with its operation and effects of Ransomware and to contemplate reasonable and legitimate responses to Ransomware attacks. Despite the intervening decades, and although Ransomware as a process and business are (somewhat) better understood, the legal implications of Ransomware attacks are still up for debate, and there is no simple answer to the question of how Ransomware victims can, or should, deal with an attack.

P3 This digital menace poses constantly evolving threats, which adds to the challenges victims confront when attempting to implement current guidance and benchmarked response efforts to Ransomware. These challenges are not only rooted in functionality and potential damage, but also due to the emergence of a viable business model facilitating Ransomware's exponential growth as a tool for criminals. We will explore these challenges by providing an overview of Ransomware's development and spread and then examining the current, albeit unsettled, legal landscape surrounding Ransomware attacks and victim responses, to consider what the future might hold for regulation in this space.

II. A HISTORY OF RANSOMWARE

P4 As noted above, Ransomware has been around in one form or another for at least ten years, [6] and as early as 1989 in the U.S. [7] and Europe. [8] The first recorded example was biologist Joseph Popp's "AIDS Trojan": Popp developed the virus and "passed 20,000 infected floppy disks out at the 1989 World Health Organization's AIDS conference." [9] Ransomware subsequently faded as a notable security concern for more than a decade before making another brief appearance in 2005. [10] Then, in the wake of an economic recession, Ransomware came back with a vengeance, making a dramatic entrance as it "resurged in 2013;" [11] it has continued to flourish ever since. Interestingly, Ransomware's recent reemergence may be explained, in part, by the success of other hacking efforts. The historical model for the most obvious cybercrimes had been stealing and selling data (usually credit card numbers), but this fraud became so prevalent that the going rate for stolen payment card information has dropped precipitously over the past five years. [12] In response, "[t]o keep cybercrime profitable, criminals needed to find a new cohort of potential buyers, and they did: all of us." [13]

---

[5] Robert E. Litan, *Law and Policy in the Age of the Internet*, 50 DUKE L.J. 1045, 1045 (2001).

[6] *See* Amin Kharraz et al., *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, in* DIMVA 2015 PROCEEDINGS OF THE 12TH INTERNATIONAL CONFERENCE ON DETECTION OF INTRUSIONS AND MALWARE, AND VULNERABILITY ASSESSMENT 3 (Springer 2015).

[7] *See* James Scott & Drew Spaniel, *supra* note 2, at 4.

[8] NICOLE VAN DER MEULEN ET AL., EUROPEAN PARLIAMENT POLICY DEP'T FOR CITIZENS' RIGHTS & CONSTITUTIONAL AFFAIRS, CYBERSECURITY IN THE EUROPEAN UNION AND BEYOND: EXPLORING THE THREATS AND POLICY RESPONSES 35 (2015), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf, https://perma.cc/6M58-B4TW.

[9] James Scott & Drew Spaniel, *supra* note 2, at 6.

[10] *See id.*

[11] *See* VAN DER MEULEN, *supra* note 8, at 35.

[12] *See* Josephine Wolff, *The New Economics of Cybercrime*, THE ATLANTIC (June 7, 2016), http://www.theatlantic.com/business/archive/2016/06/ransomware-new-economics-cybercrime/485888/, https://perma.cc/5L3U-47CT.

[13] *Id.*

P5 Although experts rightly emphasize the significant problem Ransomware presents today, the risks have not always been so grave in the hostage-software industry. As Doug Pollack noted, "ironically, until [the 2005 resurgence], most [Ransomware] was fake. Fraudulent spyware removal tools and performance optimizers scared users into paying to fix problems that didn't really exist." [14] Regardless, most present-day (and, likely, future) Ransomware *is* serious business, both in the effects it has on victims and in the underground infrastructure that buttresses Ransomware's propagation. Moreover, the scourge of Ransomware is growing steadily, with some researchers noting 500% yearly increases. [15] Other experts focus on the exponential reach of Ransomware, noting that it "infects one computer but...often spreads across network drives to infect other computers as well." [16]

P6 In the face of an inarguably immense and expanding problem, an understanding of the relevant legal issues is crucial for practitioners who will encounter Ransomware and its effects. That said, evaluating the applicable legal framework requires knowledge of Ransomware's mechanics, which may vary widely by the type, source, and purpose of the Ransomware--not to mention the specific effects it may have on a given organization.

III. RANSOMWARE AS A PROCESS

P7 Malware is malicious software, but that category "encompasses a wide range of program types including viruses, worms, logic bombs, Trojan horses, keyloggers, zombie programs, and backdoors." [17] One subcategory of Malware is "Scareware," or Malware that "takes advantage of people's fear of revealing their private information, losing their critical data, or facing irreversible hardware damage." [18] Ransomware is a subset of Scareware; specifically a "category of malicious software which, when run, disables the functionality of a computer in some way," [19] making it essentially "a digital version of hostage taking." [20] Ransomware is also classified as a type of viral software, which is software that may be grouped into separate "families" and differentiated by whether it presents only the superficial trappings of a threat or poses an actual problem. [21] We may divide the types of Ransomware that pose an actual threat into two main groups: "one-off" variants used in an ad-hoc fashion, and software that serves as an extension of the broader criminal infrastructure into which victims pay their ransom.

A. Locker Ransomware

---

[14] DOUG POLLACK, RANSOMWARE 101: WHAT TO DO WHEN YOUR DATA IS HELD HOSTAGE 7 (2016) (ebook), *http://lpa.idexpertscorp.com/acton/attachment/6200/f-051f/1/-/-/-/-/IDE_eBook_Ransomware_082616_v1.pdf?cm_mmc=Act-On%20Software-_-email-_-ID%20Experts%20Download%20-%20Ransomware%20101%3A%20What%20to%20Do%20When%20Your%20Data%20is%20Held%20Hostage-_-Download%20Now&sid=TV2:dA7ip6myT*, *https://perma.cc/327S-TXFL*.

[15] *See* Kharraz, *supra* note 6, at 1, 4.

[16] *See* Azad Ali et al., *Recovering from the Nightmare of Ransomware -- How Savvy Users Get Hit with Viruses and Malware: A Personal Case Study*, 17 ISSUES IN INFORMATION SYSTEMS 58, 61 (2016).

[17] Robert J. Kroczynski, *Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited*?, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 817, 823 (2008).

[18] *See* Kharraz, *supra* note 6, at 1.

[19] Gavin O'Gorman & Geoff McDonald, *Ransomware: A Growing Menace*, SYMANTEC CORP. (2012) at 2, *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf*, *https://perma.cc/F6UF-UDUL*.

[20] Eric Jardine, *A Continuum of Internet-Based Crime: How the Effectiveness of Cybersecurity Policies Varies across Cybercrime Types*, RESEARCHGATE, 10 (Jan. 2016), *reprinted in* RESEARCH HANDBOOK ON DIGITAL TRANSFORMATIONS 421 (F. Xavier Olleros & Majinda Zhegu eds., 2016).

[21] *See* Kharraz, *supra* note 6, at 2.

P8 Beginning with the functional mechanics of the software, Ransomware attacks can be segregated by form. Early variants [22] were primarily *Locker* Ransomware, and were identified as such (e.g., WinLocker, which would lock up a user's screen, and Master Boot Record, which would interrupt a user's normal operating system). [23] The Locker approach "restricts user access to infected systems by locking up the interface or computing resources within the system," [24] thereby blocking off access to the computer or denying access to files. [25] Locker Ransomware may display "a message that demands payment to restore functionality," [26] such that it appears similar to the other Ransomware variants discussed below, but operates quite differently.

P9 If the victim's operating system is imagined as a storage unit, where the worth of the operating system lies in the items contained within the unit, Locker Ransomware operates by effectively changing the lock on the door, or, in some cases, changing the mechanism by which the lock engages. The items within the storage unit remain untouched, and the victim is asked to pay to have the door unlocked (or to have the locking mechanism restored to its original form), but victims in such Locker Ransomware cases have other options for regaining access. For example, they can try to bypass the door by (metaphorically) drilling out the lock, taking the door off its hinges, or just removing the walls from around the unit's contents.

B. Crypto Ransomware

P10 Cryptographic approaches to Ransomware operate differently, though the initial message--pay us or you cannot access your data--looks the same at first blush. Rather than focusing solely on the lock, however, these variants [27] employ a Crypto Ransomware or CryptoLocker approach. [28] Here, the Ransomware "encrypts files on the target system so that the computer is still usable, but users can't access their data." [29] This type of Ransomware typically "uses RSA 2048 encryption to encrypt files," making "cracking the lock" to avoid paying ransom an impossibility; for an average desktop computer, this approach would take "around 6.4 quadrillion years." [30]

P11 Continuing with the storage unit metaphor, a Crypto Ransomware approach may or may not tamper with the lock on the front door. Instead, Crypto Ransomware sizes up each item within the unit, systematically determining the relative value of the files to the user. These may include, for example, unstructured data comprised of user photos, Word documents, Excel files, or PDFs. Once those files are identified by extension, the program goes to

---

[22] *See, e.g.*, William Largent, *Ransomware: Past, Present, and Future*, TALOS BLOG (Apr. 11, 2016, 9:01 AM), http://blog.talosintel.com/2016/04/ransomware.html, https://perma.cc/QU27-WDRK (last visited Feb. 6, 2017).

[23] *See* Ian T. Ramsey & Edward A. Morse, Cyberspaxe Law Comm. Winter Working Grp., Ransoming Data: Technological and Legal Implications of Payments for Data Privacy 4-5 (Jan. 29-30, 2016) (unpublished manuscript) (on file with author), http://www.stites.com/uploads/learning-center/Ramsey_Ransoming-data_Jan2016.pdf, https://perma.cc/H4BZ-UHY3.

[24] Pollack, *supra* note 14, at 7.

[25] *See* Largent, *supra* note 22.

[26] *See* O'Gorman & McDonald, *supra* note 19, at 2.

[27] *See, e.g.*, Largent, *supra* note 22.

[28] *See id.*

[29] Doug Pollack, *Trading in Fear: The Anatomy of Ransomware*, ID EXPERTS (May 2, 2016), https://www2.idexpertscorp.com/blog/single/trading-in-fear-the-anatomy-of-ransomware, https://perma.cc/7VTU-5QAC.

[30] ADAM ALESSANDRINI, RANSOMWARE HOSTAGE RESCUE MANUAL 2, (2015), http://resources.idgenterprise.com/original/AST-0147692_Ransomware-Hostage-Rescue-Manual.pdf, https://perma.cc/9V7T-L4YA.

work, encrypting each file and rendering it unusable pending payment of the ransom--unless, as we discuss below, (1) the user can find a workaround solution online; or (2) the ransom *is* paid but no key is provided.

P12 When it comes to Crypto Ransomware, there is no option to drill out the lock, take the door off the hinges, or tear down the wall; each file is locked up separately and indefinitely. [31] Accordingly, this type of Ransomware poses a very different kind of threat and, as such, is handled quite differently by experienced security professionals tasked with solving the problem.

P13 Crypto Ransomware doesn't stop there. Certain variants add insult to injury, as some may, "while encrypting files, search[] and steal[] [B]itcoins from the user." [32] Others, called "Doxware," may focus on areas normally associated with user privacy such as conversations, photos, and other sensitive files; and threaten to release them publicly unless the ransom is paid. [33] Still another form of Crypto Ransomware, Shadowlock, "forces users to complete consumer surveys of products and services as the ransom payment." [34]

P14 Although Ransomware's efficacy has improved over the decades since its introduction, many earlier forms are still in use. [35] This may be due in part to its inherent longevity, as one key element of older Ransomware's functionality is the malicious way in which its self-propagating features make it incredibly difficult to eliminate. Some legacy Ransomware variations are no longer in circulation, but certain "[m]alware that was released years--in some cases, decades--ago is still alive and well today," [36] making awareness of modern Ransomware's progenitors required knowledge for practitioners active in this space.

C. Ransomware Delivery

P15 Despite the automated nature of Ransomware's self-propagation, the spread of most Ransomware is still a personal process that relies on human error. [37] The FBI notes specifically that "Ransomware is frequently delivered through spear phishing emails" to end users. [38] Other common methods of installing Ransomware are "exploit kits," [39] "Web exploits and drive-by downloads," [40] "infected removable drives, infected software

---

[31] Considerations associated with quantum computing and decryption are outside the purview of this paper.

[32] Ramsey & Morse, *supra* note 23, at 5.

[33] Chris Ensey, *Ransomware Has Evolved, And Its Name Is Doxware*, DARKREADING (Jan. 4, 2017, 07:30 AM) http://www.darkreading.com/attacks-breaches/ransomware-has-evolved-and-its-name-is-doxware/a/d-id/1327767, https://perma.cc/VGJ6-HUHD (noting also that this would be one way of getting back access to at least some of the hostage files).

[34] *Technical Intricacies of Ransomware and Safeguarding Strategies*, FALL 2016 E-NEWSLETTER (Digital Mountain, Santa Clara, C.A.), 2016, at 1, http://digitalmountain.com/enews/FALL_2016_Article2.pdf, https://perma.cc/8CKR-3Q3A.

[35] *See* Largent, *supra* note 22.

[36] *Id.*

[37] *See id.*

[38] *See* U.S. DEP'T OF JUSTICE, PROTECTING YOUR NETWORKS FROM RANSOMWARE 2, https://www.justice.gov/criminal-ccips/file/872771/download, https://perma.cc/3GT6-ARH.

[39] *See* Largent, *supra* note 22, at 1.

[40] *See* O'Gorman & McDonald, *supra* note 19, at 4.

installers," [41] and "mass phishing campaigns." [42] In a "mass phishing campaign," [43] malware is "installed on a user's computer without their knowledge when that user browses to a compromised website," [44] and is using "outdated browsers, browser plugins, and other software." [45] These techniques may be referred to as "malvertising" where "[c]ybercriminals leverage compromised advertising networks to serve malicious advertisements on legitimate websites which subsequently infect the visitors...[later] redirecting the user to an Exploit Kit (EK) landing page." [46]

P16 In addition to leveraging self-propagation, Ransomware schemes also may rely on the "spray and pray" technique, or sending out massive quantities of malware-infected emails in hopes of hitting "as many individual targets...as quickly as possible" by virtue of sheer volume. [47] Still other types of Ransomware have begun to deploy an even more personal approach, tailoring messages to appear as genuine as possible; often through social engineering research used to gain knowledge of a company's operational structure, invoicing and remittance practices, and even individuals' writing styles. [48] Increasingly, "e-mails are highly targeted to both the organization and individual, making scrutiny of the document and sender important to prevent exploitation." [49]

D. Personality and Psychology

P17 The customization of these programs is reflected in a variety of features that are now common to Ransomware schemes. For example, certain programs display multiple language options so "language is not a barrier to payment, [allowing] the user [to] access ransom instructions in English, French, German, Russian, Italian, Spanish, Portuguese, Japanese, Chinese and Arabic" [50] and making sure that the Ransomware "experience" is appropriately localized for the victim. [51] Once the Ransomware is downloaded, it disables the victim's machine "by disallowing execution of various programs," demanding ransom, and even "using local police images" --the program

---

[41] *See Practical Steps to Thwart Ransomware and other Cyberbreaches*, YOURABA (Dec. 2016), http://www.americanbar.org/publications/youraba/2016/december-2016/be-prepared-to-thwart-ransomware-and-other-cyber-attacks.html, https://perma.cc/U5G4-VX97.

[42] *See* Largent, *supra* note 22.

[43] *Id.*

[44] *See* O'Gorman & McDonald, *supra* note 19, at 4.

[45] FED. BUREAU OF INVESTIGATION, RANSOMWARE, www.blockchainalliance.org/docs/Ransomware_e-version.pdf, https://perma.cc/66XL-V4J7.

[46] Deepen Desai, *Malvertising, Exploit Kits, ClickFraud & Ransomware: A Thriving Underground Economy*, ZSCALER (Apr. 21, 2015), https://www.zscaler.com/blogs/research/malvertising-exploit-kits-clickfraud-ransomware-thriving-underground-economy, https://perma.cc/C4PN-TM4C.

[47] *See* Largent, *supra* note 22.

[48] *See Ransomware on the Rise: Norton Tips on How to Prevent Getting Infected*, NORTON BY SYMANTEC, https://us.norton.com/ransomware/article, https://perma.cc/7MZU-XYVU.

[49] *See* FED. BUREAU OF INVESTIGATION, *supra* note 45.

[50] Ramsey & Morse, *supra* note 23, at 5.

[51] *See* Azad Ali et al., *supra* note 16, at 62.

geo-locates the user's internet protocol address and associates that address with location-specific law enforcement decals and insignia deployed from a central command-and-control server. [52]

P18 In connection with this locality-based personalization, Ransomware may use psychological tactics to induce guilt or shame in individual victims. [53] For example, ransom notes may include salacious details to frighten users, sometimes claiming that the victim has violated federal statutes and/or threatening imprisonment for alleged visits to websites "containing pornography, child pornography, zoophilia and child abuse." [54] These ransom notes are then spread throughout the computer's operating system, often propagating hundreds of copies on a given computer to ensure the user's attention is drawn to the threat. [55]

P19 Alternatively, "some versions of Ransomware are now designed to seek out the files on a victim's computer that are most likely to be precious, such as a large number of old photographs, for example, tax filings, or financial worksheets." [56] Other variants "just delete[] files instead of encrypting them." [57] Finally, some "variants display a countdown timer to the victim, threatening to delete the key/decryption tool if payment is not received before the timer reaches zero or, in other cases, increase the price of the ransom." [58]

P20 Even setting aside the nuances of these personal approaches, it is nearly impossible for security experts to keep pace with Ransomware advances generally, as "hackers are releasing over 100,000 new [R]ansomware variants daily," [59] and "'evil genius' [R]ansomware ideas are 'coming out on a regular basis.'" [60] Perhaps even more challenging for law enforcement and security specialists, the level of technological expertise required to engineer a Ransomware attack has decreased significantly; at this point, deploying Ransomware is "relatively low budget, low stakes, and [doesn't] require much skill to pull off." [61] Indeed, in one instance, a recent drop in price to US$ 39 for Ransomware software concerned experts who believed "the low price coupled with its potency could trigger a wave of new infections." [62]

P21 Evolving with the times, recent Ransomware variants have focused on smartphones and other connected devices, including those that are a part of the "Internet of Things." [63] The first instances of "mobile-focused

---

[52] O'Gorman & McDonald, *supra* note 19, at 5.

[53] *See* Haley S. Edwards, *A Devastating Type of Hack Is Costing People Big Money*, TIME (Apr. 21, 2016), http://time.com/4303129/hackers-computer-ransom-ransomware/, https://perma.cc/AAQ3-52BB.

[54] O'Gorman & McDonald, *supra* note 19, at 2.

[55] *See* Ali et al., *supra* note 16, at 61-62.

[56] Edwards, *supra* note 53.

[57] Tom Spring, *Dirt Cheap Stampado Ransomware Sells on Dark Web for $ 39*, THREATPOST (July 14, 2016, 12:35 PM), https://threatpost.com/dirt-cheap-stampado-ransomware-sells-on-dark-web-for-39/119284/, https://perma.cc/A4HS-ZF3H.

[58] Largent, *supra* note 22.

[59] Pollack, *supra* note 14, at 5.

[60] Ricci Dipshan, *Danger Ahead: 3 New Ransomware Developments in 2016; From Hybrid Ransomware to Attacks on Mobile Devices and New Entrants in the Field, Experts Warn of a Difficult Year Ahead*, LAW TECH. NEWS (May 31, 2016).

[61] Edwards, *supra* note 53.

[62] Spring, *supra* note 57.

[63] *See, e.g.*, Antigone Peyton, *A Litigator's Guide to the Internet of Things*, 22 RICH. J. L. & TECH. 9, P 1 (2016), http://jolt.richmond.edu/v22i3/article9.pdf, https://perma.cc/VSZ7-85LE.

Ransomware came out in 2013," [64] buoyed in part "by the practice of users downloading pirated apps from unsanctioned app stores." [65] As noted by another commentator, "[R]ansomware criminals can achieve some profit from targeting any system: mobile devices, personal computers, industrial control systems, refrigerators, portable hard drives, etc. The majority of these devices are not secured in the slightest against a [R]ansomware threat." [66]

IV. THE BUSINESS OF RANSOMWARE

> You always wanted a Ransomware but never wanted two pay Hundreds of dollars for it? This list is for you!?? Stampado is a cheap and easy-to-manage ransomware, developed by me and my team. It's meant two be really easy-to-use. You'll not need a host. All you will need is an email account. [67]

P22 The mentality behind Ransomware seems to have deep-rooted cultural underpinnings, likened by some authors to medieval roadways that became host "to travelling footpads referred to as highwaymen." [68] Methodologically, the purveyors of Ransomware bear little resemblance to hackers "who attempt to exfiltrate or manipulate data where it is stored, processed, or in transmission;" instead, "ransomware criminals only attempt to prevent access to the data." [69] In short, Ransomware aims to disrupt.

P23 Ransomware differs from many other types of hacking on a number of levels. It has been called a "business model" [70] that has "quickly risen to dominance" [71] within the "cybercriminal market in the past few years" [72] and has "emerged as one of the most serious online threats facing businesses." [73]

P24 Often, a Ransomware attempt betrays the fact that its author "lack[s] the technical complexity to perform successful attacks;" [74] some versions have been described as lacking technical savvy, and others as "not very well developed" beginner-level efforts. [75] Perhaps because of a general lack of know-how, and Ransomware's reputation as offering "easier money than hacking into personal information to use for identity theft," [76] a cottage industry has mushroomed. Certain criminals "now have the resources to hire professional developers to build

---

[64] *See* VAN DER MEULEN, *supra* note 8, at 45.

[65] Dipshan, *supra* note 60.

[66] *See* Scott & Spaniel, *supra* note 2, at 4.

[67] Spring, *supra* note 57.

[68] Scott & Spaniel, *supra* note 2, at 3.

[69] *See id.* at 4.

[70] *See* Jon Neiditz, *Ransomware in Society and Practice*, PRACTISING LAW INST. 39, 41.

[71] *Id.*

[72] *Id.*

[73] Ben Rossen, *Ransomware -- A Closer Look*, FED. TRADE COMM'N (Nov. 10, 2016, 11:05 AM), *https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look*, *https://perma.cc/3HX4-NDE3*.

[74] Kharraz, *supra* note 6, at 2.

[75] Dipshan, *supra* note 60.

[76] THOMPSON INFORMATION SERVICES, *Malware Attack Causes System Shutdown at Medstar*, 15 NO. 4 GUIDE MED. PRIVACY & HIPAA NEWSL. 2, at 1 (May 2016) [hereinafter *Malware Attack*]

increasingly sophisticated malware" on their behalf. [77] Providers, "usually based in Russia, Ukraine, Eastern Europe and China, have begun licensing what's known as 'exploit kits'--all-inclusive Ransomware apps--to individual hackers for a couple hundred dollars a week," [78] or even "[US]$ 50 for a set period time of use," [79] frequently taking a "cut of the profits from payouts." [80]

P25 Known as "Ransomware-as-a-service" (or RaaS), there are now "products, such as CerberRing, which provide[] less-tech savvy criminals a corridor into cybercrime, and yield[] criminal affiliates (often tasked with distributing the [R]ansomware) a healthy portion of the profits." [81] Interestingly enough, because Ransomware is such big business, some Ransomware enterprises actually offer "customer service which victims can contact to negotiate" [82] and similar structures that make both launching the attacks, and paying the ransoms, easier. [83]

P26 Some commentators note that there is "some honour among thieves," where "hackers almost always honour their word and provide the encryption key to those who make timely online payments." [84] Others disagree, noting that a decision to pay does not consistently restore functionality, and "[t]he only reliable way to restore functionality is to remove the malware." [85] For many this is truly unfortunate, as "[t]he costs of downtime often exceed the cost of ransom." [86]

P27 Ransomware infrastructure has "begun to mimic the way modern software is developed: there are criminal engineers and manufacturers, retailers, and 'consumers'--[those] hackers on the lookout for the newest, most effective product." [87] In some cases, when a ransom is paid functionality may be restored but in an inconsistent manner (e.g., accounting data may be returned, but mapped drive data is not); in at least one of those cases, the victim determined that the "help" offered by the Ransomware attacker could instead lead to the loss of more data. [88]

P28 Ransomware may be preferred by criminals because it cuts out the middle-man. [89] It bypasses many of the annoyances associated with hacking to steal data that then must be monetized. Where "intellectual property, or

---

[77] Rossen, *supra* note 73.

[78] Edwards, *supra* note 53.

[79] Spring, *supra* note 57.

[80] Largent, *supra* note 22.

[81] *See Technical Intricacies of Ransomware and Safeguarding Strategies*, DIGITAL MOUNTAIN (Fall 2016) http://digitalmountain.com/enews/FALL_2016_Article2.pdf, https://perma.cc/QV3V-ESJQ.

[82] Pollack, *supra* note 14, at 14.

[83] *See* Brian Krebs, *CryptoLocker Crew Ratchets Up the Ransom*, KREBS ON SECURITY (Nov. 6, 2013, 12:13 AM), http://krebsonsecurity.com/tag/cryptolocker-decryption-service/, https://perma.cc/7369-JSKT.

[84] Jardine, *supra* note 20, at 10.

[85] O'Gorman & McDonald, *supra* note 19, at 2.

[86] Pollack, *supra* note 14, at 5.

[87] Edwards, *supra* note 53.

[88] *See* Azad Ali et. al., *supra* note 16, at 64.

[89] *See* SENTINEL ONE, *Ransomware is Here: What You Can Do About It?* 2, https://go.sentinelone.com/rs/327-MNM-087/images/Sentinel%20One_Ransomware%20is%20Here.pdf, https://perma.cc/3H46-QJCB.

other sensitive information that is stolen outright....is often 'fenced' on the Dark Web, then the buyer has to turn it into a false identity that can be used to fraudulently obtain goods or services." [90] In contrast, Ransomware has victims who "pay the criminal directly, the payment happens within hours or days in untraceable currency, and there is no chain of custody to point to the criminals because the data stays on the victim's system the whole time." [91] Indeed, deploying Ransomware is especially convenient for criminals, as its operation "often means dealing not with a small group of fellow criminals, but instead with a much larger population of lay users who are unlikely to disappear behind bars." [92]

V. RANSOMWARE'S DIRECT IMPACT

P29 In some cases, specific industries have been singled out as popular targets. For instance, at the time of writing, "[R]ansomware is the dominant current information security threat to health care providers." [93] Ransomware may target "victims like healthcare providers whose complex independent networks and critical need for real-time information can make reliance on backups difficult and potentially life-threatening." [94] These types of targets ("hospitals in particular" but also "other firms heavily dependent on computers" [95]) tend to focus on paying off the attacker to make the problem go away, whereas other types of companies may be amenable to "resisting the attack and rebuilding entire systems." [96] If the demands are not met, in the most extreme examples, a victim might be "forced back into the 1980s: digital typewriters, notebooks, fax machines, post-it notes, paper checks and the like." [97] In the face of these challenges, many organizations and individuals simply pay. Some do so without fanfare, and experts claim it "would shock you [] how many companies have quietly gone ahead and paid for information to be returned." [98] Others, like PayPal, have made public the fact that they will pay for stolen data to protect their customers. [99]

P30 One commentator noted that attorneys increasingly are "targets of [R]ansomware;" in the past several years, a number of "large and small law firms in the United States and Canada have had their office computer systems compromised by [R]ansomware." [100] Some professionals "suspect that paying gets you listed on the Dark Web as

---

[90] Pollack, *supra* note 14, at 5.

[91] *Id.*

[92] Wolff, *supra* note 12.

[93] Neiditz, *supra* note 71, at 7 (citing Danny Palmer, *Ransomware is Now the Biggest Cybersecurity Threat*, ZDNET (May 6, 2016), http://www.zdnet.com/article/ransomware-is-now-the-top-cybersecurity-threat-warns-kaspersky/, https://perma.cc/84XM-57M3).

[94] *Id.* at 9.

[95] Merrion, *supra* note 4.

[96] *Id.*

[97] Largent, *supra* note 22.

[98] Wolff, *supra* note 12.

[99] *See* Sean Sposito, *PayPal, OthersBuy Stolen Data from Criminals to Protect Users*, SAN FRANCISCO CHRON. (Jan. 8, 2016), http://www.sfchronicle.com/business/article/PayPal-others-buy-stolen-data-from-criminals-to-6744699.php, https://perma.cc/XLE9-AX3Q.

[100] Daniel Crothers, *Cybersecurity for Lawyers -- Part IV: Is Payment of Ransom in Your Budget?*, 63 THE GAVEL 24, 24 (2016).

an easy target, setting you up for more attacks." [101] At least in some cases, the FBI appears to agree. [102] Ransomware's effects are not just monetary, as the loss of the files themselves (or the cost of ransom) may be eclipsed by the loss of "client trust, relationships, and reputation." [103]

VI. RANSOMWARE'S INDIRECT IMPACT

P31 One commentator notes that Ransomware is an exception (and perhaps portends a wave of such exceptions) to the traditional "data security breach" concept with which we have all become familiar. [104] Whereas a traditional "breach" typically entails the acquisition of data, Ransomware allows wrongdoers to control, damage, and interrupt systems; deny access to data; and destroy or otherwise harm the data's integrity--all *without* actual acquisition of the data. [105]

P32 Although some contend that "no information is actually stolen during a [R]ansomware attack," [106] others argue that falling victim to Ransomware "could also be considered a data breach, even though the data never leaves the victim's systems." [107]

P33 The issue of whether Ransomware constitutes a breach was raised at the 2016 Healthcare Compliance Association conference. [108] There, Iliana Peters of the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) "pointed out that HIPAA regulations define a data breach as 'impermissible acquisition, access, use or disclosure of PHI [protected health information](paper or electronic) which compromises the security or privacy of the PHI.'" [109] Additional HIPAA guidance from the OCR also notes that some Ransomware may "exfiltrate" the data, [110] which further complicates a simple explanation for the mechanics of a Ransomware attack. The OCR also noted that "[h]ospitals and other healthcare providers hit by [R]ansomware attacks should notify affected individuals, the federal government and perhaps the news media unless there is a 'low probability' any personal health information was disclosed." [111] That "guidance makes clear that a [R]ansomware attack

---

[101] Pollack, *supra* note 14, at 11 (quoting unnamed consultant "D").

[102] *See* Mathew J. Schwartz, *Please Don't Pay Ransoms, FBI Urges*, DATA BREACH TODAY (May 4, 2016), http://www.databreachtoday.com/blogs/please-dont-pay-ransoms-fbi-urges-p-2120, https://perma.cc/8ZND-KM2J.

[103] *See* A.B.A., *Practical steps to thwart ransomware and other cyberbreaches*, YOURABA (Dec. 2016), http://www.americanbar.org/publications/youraba/2016/december-2016/be-prepared-to-thwart-ransomware-and-other-cyber-attacks.html, https://perma.cc/LFT2-UP9E.

[104] *See* Neiditz, *supra* note 70, at 41.

[105] *See id.*

[106] Jardine, *supra* note 20, at 10-11.

[107] DOUG POLLACK, RANSOMWARE 101: WHAT TO DO WHEN YOUR DATA IS HELD HOSTAGE, 5 (2016) (ebook).

[108] *See id.*

[109] *Id.*

[110] *See Fact Sheet: Ransomware and HIPAA*, DEPT. OF HEALTH & HUM. SERV., http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf, https://perma.cc/G6ZV-S87S (last visited Feb. 8, 2017).

[111] Paul Merrion, HHS Clarifies When Ransomware Attacks Trigger HIPAA Notification, CQ ROLL CALL, July 13, 2016, 2016 WL 3709987 [hereinafter *HHS Clarifies*].

usually results in a 'breach' of healthcare information under the HIPAA Breach Notification Rule," noted OCR's Executive Director, Jocelyn Samuels. [112]

P34 In contrast, some argue that data breach notification statutes were implemented with a focus on informing citizens that their personal information may have been compromised, offering "valuable warnings to assist victims in protecting themselves" and otherwise corralling information that has been set loose in the outside world. [113] The July 2016 HHS guidance also indicates that the question of "whether notification is required comes down to a 'fact-specific determination.'" [114] In some cases, a forensic investigation may provide evidence to support a company's conclusion that a ransomware attack did not expose any personal information, even if the incident resulted in a system shutdown or other functional difficulties. Many healthcare entities have reached this same conclusion under HIPAA.

VII. RESPONSE TO RANSOMWARE

P35 Although the following discussion examines conventional best practice approaches for dealing with Ransomware, but the preceding section should signal that there is no one-size-fits-all solution. As with many computer infections, a typical initial response to Ransomware may be to restart the computer in "safe mode" in an effort to disable a number of programs that might be causing issues. [115] In the case of Ransomware, however, this approach may backfire, allowing the malicious software to flourish by un-loading antivirus programs that otherwise may have stopped it. [116]

P36 The next step in the response protocol is for victims to identify which "strain" of Ransomware they are dealing with, and then determine whether an "applicable decryption method" may be readily available to help unlock or decrypt files. [117] Whether this approach will be successful depends on the sophistication of the Ransomware. Certain generic, readily available strains that are still freely disseminated among would-be hackers may be defeated with relative ease, and the fact that a given strain of Ransomware is still in circulation is not proof of its viability or effectiveness. [118] To give one example, "the makers of Jigsaw ransomware have continued their assault against victims despite the fact its encryption scheme has been defeated by security researchers." [119]

P37 If these initial efforts are unsuccessful, certain victims may be inclined to pay the ransom. Experts may caution against paying the ransom prematurely, but for many, a relatively paltry Ransomware demands (demands often

---

[112] Jocelyn Samuels, *Your Money or Your PHI: New Guidance on Ransomware*, OPENHEALTH NEWS, July 11, 2016, http://www.openhealthnews.com/news-clipping/2016-07-11/your-money-or-your-phi-hhs-issues-new-guidance-ransomware, https://perma.cc/Q7P7-P8WL.

[113] John Neiditz & David Cox, *Beyond Breaches: Growing Issues In Information Security*, INTEGRO (2016), https://integrogroup.com/uploads/white_papers/06_16_Beyond-Breaches.pdf, https://perma.cc/U5EJ-SAC8.

[114] HHS Clarifies, supra note 111.

[115] *See generally* Azad Ali et. al., *supra* note 16, at 66 (describing the authors' personal experience with ransomware mechanisms).

[116] *See id.*

[117] *See* Adam Alessandrini, *Ransomware Hostage Rescue Manual*, KNOWBE4 (2015) at 8, http://resources.idgenterprise.com/original/AST-0147692_Ransomware-Hostage-Rescue-Manual.pdf, https://perma.cc/KNS8-BT5N.

[118] *See id.* at 7.

[119] Tom Spring, *Dirt Cheap Stampado Ransomware Sells on Dark Web for $ 39*, THREATPOST, July 14, 2016, https://threatpost.com/dirt-cheap-stampado-ransomware-sells-on-dark-web-for-39/119284/, https://perma.cc/2LAV-63HE.

range from US$ 200 to US$ 2,000) may be seen as "nuisance fee" more than anything else. [120] The "To Pay or Not to Pay" [121] characterization of a standard response to Ransomware is apt, though this decision-making process may mean waiting to decide until after an initial deadline is extended. [122] Waiting may result in a doubling of the ransom [123] or even an exponential increase--up to US$ 20,000 in some instances. [124] And in some cases there really is no choice. As noted in a recent report, "[f]or variants of [R]ansomware that rely on types of strong asymmetric encryption that remain relatively unbreakable without the decryption key, victim response is sharply limited to pay[ing] the ransom or los[ing] the data. No security vendor or law enforcement authority can help victims recover from these attacks." [125]

P38 Paying a ransom may, therefore, make logical sense, given that "Ransomware attacks, especially those against individual users, only demand a few hundred dollars at most from the victim" and "[f]rom law enforcement's perspective, a home burglary results in greater loss than a singular [R]ansomware attack." [126] At least one commentator noted cynically that, because "[s]ecurity has always been a business decision, [s]ome companies would rather pay a lower fee for ransom than pay for the cost of having a robust security stance." [127] Others note that "to save money, some organizations don't include all their important files in their backups, or don't run their backups often enough." [128]

P39 However, notwithstanding the low dollar value of most demands, taken in the aggregate, these attacks cost real money. "[L]osses for victims from a single strain of the CryptoWall malware were close to $ 18 million," [129] and another Ransomware attacker earned roughly $ 1 million. [130] Given that "nearly 30 percent of CryptoLocker and CryptoWall victims pay the ransom," [131] there remains the concern that "hackers [will] continue to ask for

---

[120] *See* Crothers, *supra* note 100 at 24.

[121] *See* Scott & Spaniel, *supra* note 2, at 3.

[122] *See* Ondrej Kehel, *Ransomware: To Pay or Not To Pay*, LEXISNEXIS, Aug. 16, 2016, https://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2016/08/16/ransomware-to-pay-or-not-to-pay.aspx, https://perma.cc/V2JJ-YHPT.

[123] *See* Azad Ali et. al., *supra* note 16, at 64.

[124] *See* Jardine, *supra* note 20, at 10.

[125] Scott & Spaniel, *supra* note 2, at 4.

[126] *Id.* at 5.

[127] Michael Sutton, *Big Business Ransomware: A Lucrative Market in the Underground Economy*, DARKREADING, July 1, 2016, http://www.darkreading.com/vulnerabilities--threats/big-business-ransomware-a-lucrative-market-in-the-underground-economy/a/did/1326144, https://perma.cc/3GUA-Z8UE.

[128] Maria Korolov, *Will Your Backups Protect You Against Ransomware?*, CSO (May 31, 2016) http://www.csoonline.com/article/3075385/backup-recovery/will-your-backups-protect-you-against-ransomware.html, https://perma.cc/LM56-ZMY5.

[129] Doug Pollack, *How Ransomware Could Hold Your Business Hostage*, IDEXERTS, Apr. 29, 2016, https://www2.idexpertscorp.com/blog/single/how-ransomware-could-holdy-our-business-hostage, https://perma.cc/VK9J-B4J5.

[130] *See* Haley Sweetland Edwards, *A Devastating Type of Hack is Costing People Big Money*, TIME (Apr. 21, 2016), http://time.com/4303129/hackers-computer-ransom-ransomware/, https://perma.cc/VS8M-CDZW.

[131] Nicole van der Meulen et. al., *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, EUROPEAN PARLIAMENT at 35 (2015),

higher and higher ransoms." [132] Early payment schemes involved payment through "an SMS text message or regular call to a premium rate number" where such charges could be "as high as $ 460." [133] A second iteration of payment schemes moved to prepaid electronic payment systems such as Paysafecard, Ukash, and Moneypak, where Ransomware victims are required to purchase special PIN numbers. [134]

P40 Regardless of whether it makes business sense for victims to pay a victim to pay a given ransom, victims must also consider whether they *may* pay. Unhelpfully, regulatory authorities have expressed varying opinions on that point and have not provided definitive guidance as to whether victims should pay. The FTC notes that "[l]aw enforcement doesn't recommend paying the ransom" while warning that "it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back." [135] In contrast, Joseph Bonavolonta, the head of the FBI's Cyberand Counterintelligence Program in 2015, stated that the FBI "often advise[s] people just to pay the ransom." [136] Rick Kam, president of ID Experts, also opined that "it is often easier just to pay the ransom than to do without the data." [137] Anecdotally, the authors have heard a wide range of opinions with respect to whether paying the ransom is a sound approach. Indeed, given the exploding number of attacks and diversity of outcomes, it is increasingly challenging to offer affected companies or individuals clear recommendations on how to assess the likelihood of success when it comes to answering a Ransomware demand.

P41 In short, law enforcement guidance may boil down to a "[l]ook, we can't help you," [138] response, even if some agencies indicate that "[m]ost...including law enforcement don't condone paying the ransom," [139] and "[m]ost security vendors advise the public (who are not yet victims) to never pay the ransom and to focus on mitigation efforts instead." [140] The FBI, however, appears to be seeking "public-private partnerships," as the Bureau utilizes notifications it receives regarding Ransomware and other threats in an overall effort to build up more comprehensive forms of defense and prevention. [141]

VIII. PRACTICAL AND LEGAL CONSIDERATIONS

---

http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf, https://perma.cc/242L-VJTM (citing Richard Pinson,*Computer threat: Cryptolocker virus is ransomware*, NASHVILLE BUSINESS JOURNAL, Aug. 10, 2015 http://www.bizjournals.com/nashville/blog/2015/08/computer-threatcryptolocker-virus-is-ransomware.html, https://perma.cc/69SN-RD2Y (last visited Oct. 12, 2015)).

[132] Michael Sutton, *Big Business Ransomware: A Lucrative Market in the Underground Economy*, DARKREADING (July 1, 2016 11:20 AM) http://www.darkreading.com/vulnerabilities--threats/big-business-ransomware-a-lucrative-market-in-the-underground-economy/a/d-id/1326144, https://perma.cc/63LK-7855.

[133] O'Gorman & McDonald, *supra* note 19, at 4.

[134] *See id.*

[135] Ben Rossen, *How to Defend Against Ransomware*, FEDERAL TRADE COMMISSION, Nov. 10, 2016, https://www.consumer.ftc.gov/blog/how-defend-against-ransomware, https://perma.cc/7VVN-WG2L.

[136] Scott & Spaniel, *supra* note 2, at 5.

[137] *Malware Attack, supra* note 76, at 1.

[138] Edwards, *supra* note 54.

[139] Rossen, *supra* note 73.

[140] Scott & Spaniel, *supra* note 2, at 5.

[141] Merrion, *supra* note 4.

P42 In almost all cases, Ransomware ransom demands must be paid in a digital currency such as Bitcoin. [142] Bitcoin emerged in 2009 [143] and has had unpredictable and profound effects, particularly with respect to the underground economy. [144] For many victims, receipt of a Bitcoin ransom demand is the first time they are exposed to the term, and very few have the necessary resources available to pay such a demand in a timely manner. Others who are aware of the threat--or who have a need for Bitcoin as a payment method for unrelated reasons--may "stockpile [B]itcoins in order to pay off cyber criminals who threaten to bring down their critical IT systems." [145] To provide one public example, Hollywood Presbyterian Medical Center recently paid $ 17,000 in Bitcoin in response to a ransom demand. [146]

P43 Unfortunately, making a Bitcoin payment is not a straightforward prospect for most organizations. The process is rife with potential legal and practical problems, because the company will likely "need to buy Bitcoins from an online exchange. The exchange will require you to supply a bank account or debit card number to fund the transaction, which creates an immediate risk because Bitcoin exchanges are notorious for being hacked." [147]

P44 To add another layer of complexity, in its March 25, 2014 Virtual Currency Guide, the United States Internal Revenue Service declared that a virtual currency such as Bitcoin is considered property, not currency, and thus its use is a taxable event. [148] Further, "[a] payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property." [149] "The basis of virtual currency...is the fair market value of the virtual currency in U.S. dollars as of the date of receipt", which means that a taxpayer could end up with a taxable gain or loss, depending on the net outcome. [150]

P45 Concurrently, Ransomware perpetrators who demand Bitcoin ransoms run the risk of also violating financial services laws and regulations prohibiting the operation of unlicensed banks--or at least causing such violations.

---

[142] *See* Azad Ali et. al., *supra* note 16, at 63.

[143] *See* Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun, *Bitter to better--how to make bitcoin a better currency*, International Conference on Financial Cryptography and Data Security, pp. 399-414. Springer Berlin Heidelberg (2012). *See also, Who is Satoshi Nakamoto*, CoinDesk, Feb. 19, 2016, *http://www.coindesk.com/information/who-is-satoshi-nakamoto/*, *https://perma.cc/6JP8-NLRU*.

[144] *See generally* Andy Greenberg, *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market*, FORBES (Sept. 5, 2013), *https://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/#3cd73b93adf7*, *https://perma.cc/ZEA2-JPDR* (explaining why Bitcoin is used for underground transactions).

[145] Jamie Doward, *City Banks Plan to Hoard Bitcoins to Help Them Pay Cyber Ransoms*, THE GUARDIAN, Oct. 22, 2016, *https://www.theguardian.com/technology/2016/oct/22/city-banks-plan-to-hoard-bitcoins-to-help-them-pay-cyber-ransoms*, *https://perma.cc/PG4H-2TVL*.

[146] *See* Robert Mclean, *Hospital Pays Bitcoin Ransom After Malware Attack*, CNN, Feb. 17, 2016, *http://money.cnn.com/2016/02/17/technology/hospital-bitcoin-ransom/*, *https://perma.cc/78FT-GUMM*.

[147] Doug Pollack, *Tradable, Untraceable, Sometimes Unavoidable: The Business of Bitcoin*, ID EXPERTS, June 20, 2016, *https://www2.idexpertscorp.com/blog/single/tradable-untraceable-sometime-sunavoidable-the-business-of-bitcoin*, *https://perma.cc/VM4R-R2Y4*.

[148] *See* Ramsey & Morse, *supra* note 23, at 7.

[149] *IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property of U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*, IRS, Mar. 25, 2014, *https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance*, *https://perma.cc/JP66-2H87*.

[150] *I.R.S. Notice 2014-21 at 3,* Mar. 25, 2014, *https://www.irs.gov/irb/2014-16_IRB/ar12.html*, *https://perma.cc/MX9U-WCWN*.

[151] "[T]he U.S. Attorney for the Southern District of New York issued a press release concerning [a] criminal prosecution against Anthony R. Murgio and Yuri Lebedev for running an unlicensed Bitcoin exchange used by victims of CryptoWall [R]ansomware to pay ransoms [to their attackers] via TOR (The Onion Router)." [152] The two men were accused of having operated Coin.mx, a Bitcoin exchange service, in violation of federal anti-money laundering laws and regulations and that, "in doing so, they knowingly exchanged cash for people whom they believed may be engaging in criminal activity." [153] It is alleged that, in total, "between approximately October 2013 and January 2015, Coin.mx exchanged at least [US]$ 1.8 million for Bitcoins on behalf of tens of thousands of customers." [154] In addition, during this time, Murgio allegedly "transferred hundreds of thousands of dollars to bank accounts in Cyprus, Hong Kong, and Eastern Europe, and received hundreds of thousands of dollars from bank accounts in Cyprus and the British Virgin Islands, in furtherance of the operations of his unlawful business." [155] In doing so, the operators of Coin.mx were said to have "knowingly enabled the criminals responsible for those attacks to receive the proceeds of their crimes" thereby violating federal anti-money laundering laws, because they "never filed any suspicious activity reports regarding any of the transactions." [156]

P46 As part of its efforts to combat global terrorism, the U.S. actively works to prevent terrorists from accessing and using its financial system. [157] Payments to criminals using Ransomware to hold data hostage may run afoul of banking laws and policies as well as related statutes and regulations. Individuals and organizations choosing to make ransom payments to end Ransomware attacks could be subject to international sanctions programs administered in the U.S. by the Office of Foreign Assets Control (OFAC), though such enforcement has not yet been tested as of this writing. Under these sanctions programs, ransom payments to certain entities are illegal, as noted by Samuel Cutler:

> It's important to begin from the fact that ransom payments to [Foreign Terrorist Organizations] FTOs or Specially Designated Global Terrorists ("SDGTs") identified by [OFAC] are illegal under U.S. law. Monetary contributions to FTOs are considered material support under *18 U.S.C. 2339B,* while transfers to SDGTs are violations of economic sanctions imposed pursuant to the International Emergency Economic Powers Act ("IEEPA").
>
> Furthermore, as the Financial Action Task Force ("FATF") notes in discussion of ransom payments to the Islamic State in Iraq and the Levant ("ISIL"), "[U.N. Security Council] Resolution 2161 applies to both direct payments and indirect payments through multiple intermediaries, of ransoms to groups or individuals on the Al-Qaida Sanctions List. These restrictions apply not only to the ultimate payer of the ransom, but also to the

---

[151] *See* Ramsey & Morse, *supra* note 23, at 5.

[152] *Id.*

[153] *Manhattan U.S. Attorney Announces Charges Against Two Florida Men for Operating an Underground Bitcoin Exchange*, FBI, July 21, 2015, *https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/manhattan-u.s.-attorney-announces-charges-against-two-florida-men-for-operating-an-underground-bitcoin-exchange*, *https://perma.cc/Z85B-LT87*.

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *See* David S. Cohen, *Kidnapping for Ransom: The Growing Terrorist Financing Challenge*, COUNCIL ON FOREIGN RELATIONS, Oct. 5, 2012, *http://www.cfr.org/terrorist-financing/remarks-treasury-under-secretary-cohenkidnapping-ransom-growing-terrorist-financing-challenge/p29376*, *https://perma.cc/6X6P-NKHJ*.

parties that may mediate such transfers, including insurance companies, consultancies, and any other financial facilitators." [158]

P47 So far, the act of paying to remove Ransomware has not been prosecuted under *18 U.S.C. 2339B* [159] or IEEPA, but U.S. law enforcement officials encourage victims of Ransomware to report the attacks and are actively seeking to uncover the people behind these attacks. It remains to be seen whether a substantial Ransomware-related payment that was determined to have been made to a person or group on an OFAC list may result in legal action. [160]

P48 In addition, an Executive Order issued in April 2015 "expand[s] the [existing] sanctions regime to block the property and interests of persons engaging in 'significant malicious cyber-enabled activities'" outside of the U.S. that constitute a significant threat to the country. [161] Activities deemed significant "have the purpose or effect of" seriously harming or compromising critical infrastructure; disrupting the availability of computers and networks; and misappropriating funds, trade secrets, personal identifiers, or financial information. [162] Moreover, "[t]he blocking extends to assets of those who 'have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity [proscribed by the order] or any person whose property and interests are blocked pursuant to this order,'" which could implicate individuals and institutions that choose to pay to remove Ransomware. [163] Ransomware disrupts the availability of computers and networks, has the ability to compromise critical infrastructure, and may allow for the misappropriation of information. "Aiding" Ransomware perpetrators by acquiescing to their ransom demands could put those who pay at risk of having their own assets blocked. [164]

P49 In fact, the U.S. government's hostage policy may be instructive in determining whether a Ransomware payment is likely to be prosecuted. The government itself will not pay ransoms to release human hostages, but the relevant policy explicitly states that families will not be prosecuted for paying ransoms in exchange for hostages, even if these payments are made to FTOs or other individuals or groups on the government's sanctions lists. [165] Former President Obama noted that "no family of an American hostage has ever been prosecuted for paying a ransom for the return of their loved ones." [166] Whether that U.S. policy would extend to *photos* of an individual's

---

[158] Samuel Cutler, *Could the Administration's New Hostage Policy Leave Banks Vulnerable*?, SANCTION LAW, June 24, 2015, *http://sanctionlaw.com/could-the-administrations-new-hostage-policy-leave-banks-vulnerable/*, *https://perma.cc/5B9ZKX23*.

[159] *See* *18 U.S.C. § 2339B* (2012).

[160] *See id.*

[161] Ramsey & Morse, *supra* note 23, at 14.

[162] *See* Exec. Order No. 13,694, *80 Fed. Reg. 18,077* (Apr. 1, 2015).

[163] Ramsey & Morse, *supra* note 23, at 14 (quoting Exec. Order No. 13,694, *80 Fed. Reg. at 18078).*

[164] *See id.*

[165] *See* Cutler, *supra* note 158; *see also Statement by the President on the U.S. Government's Hostage Policy Review*, THE WHITE HOUSE OFFICE OF THE PRESS SECRETARY, June 24, 2015, *https://www.whitehouse.gov/the-press-office/2015/06/24/statement-president-us-governments-hostage-policy-review*, *https://perma.cc/W5J4-UNFK* ("[T]he United States government will not make concessions, such as paying ransom, to terrorist groups holding American hostages… At the same time, we are clarifying that our policy does not prevent communication with hostage-takers - by our government, the families of hostages, or third parties who help these families").

[166] *See Statement by the President on the U.S. Government's Hostage Policy Review, supra* note 165.

loved ones held hostage by Ransomware is an entirely different question--one that may well test the limits of the government's humanitarian leniency in this regard.

P50 Current U.S. hostage policy also offers no exemption from prosecution for organizations making or facilitating ransom payments. [167] The FBI notes in its Ransomware guidance that "by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals." [168] Moreover, intermediaries cannot be used to avoid OFAC sanctions, which include freezing assets, forfeiture of assets, preventing payment transfers, fines, and imprisonment. [169] In Ransomware attacks, it may be impossible to ascertain who exactly is holding the data hostage, which in turn prevents the victim from determining in advance whether a ransom payment could result in sanctions for the organization.

P51 Ultimately, it seems unlikely that individuals will be penalized for making small payments to regain access to personal data affected by Ransomware; enforcement is challenging on a practical level, as the anonymity of virtual currencies makes it difficult--if not impossible--to know whether payments are going to individuals or groups on sanctions lists. [170] Large organizations considering whether to pay higher amounts to meet demands from Ransomware attackers may face a more aggressive enforcement landscape. In some cases, organizations have engaged third parties to pay virtual currency ransom demands on their behalf. Ransomware payoffs and other hacking-related expenses may be funneled through intermediaries that "are often part of a larger contract for countersurveillance work, ensuring corporate accounting departments don't need to green-light individual black market buys." [171] With respect to the concept of paying ransom generally, it is worth considering the court's ruling in *United States v. Kozeny*, [172] in which the "United States District Court for the Southern District of New York [found] that only extortion or duress under the threat of *imminent physical harm* would excuse[] the conduct" (emphasis added). [173] It is difficult to imagine extending that line of reasoning to include threats to important documents or photos, especially given that industry best practices for business continuity include maintaining robust backups that would protect against just this threat. [174]

P52 As noted by some practitioners, [175] counsel's advice on preventing and responding to Ransomware attacks may implicate Model Rule 1.1 - Competence, as amended by Comment 8, where "...a lawyer should keep abreast

---

[167] *See, e.g., Manhattan U.S. Attorney Announces Charges Against Two Florida Men for Operating an Underground Bitcoin Exchange, supra* note 153. DOUBLE CHECK THIS TO SEE IF ACTUALY *18 USC 2339*

[168] *Incidents of Ransomware on the Rise: Protect Yourself and Your Organization*, FBI, April 29, 2016, *https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise*, *https://perma.cc/83FC-G2W8* (citing Federal Bureau of Investigation Cyber Division Assistant Director James Trainor).

[169] *See OFAC FAQs: Sanctions Compliance*, U.S. DEP'T OF THE TREASURY, *https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx*, *https://perma.cc/2ACP-XZ7V* (last visited Mar. 31, 2017).

[170] *See* Jardine, *supra* note 20, at 11.

[171] Sposito, *supra* note 99.

[172] *See United States v. Kozeny, 582 F. Supp. 2d 535, 540 (S.D.N.Y. 2008).*

[173] Ramsey & Morse, *supra* note 23, at 19 (emphasis added).

[174] *See* Korolov, *supra* note 128.

[175] *See, e.g.*, Ivan Hemmans & David G. Ries, *Cybersecurity: Ethically Protecting Your Confidential Data in a Breach-A-Day World* (PowerPoint), at slides 18-21, April 27, 2016, *http://www.americanbar.org/content/dam/aba/multimedia/cle/materials/2016/04/ce1604lpi.authcheckdam.pdf*, *https://perma.cc/V4T7-TAFT*.

of changes in the law and its practice, including the benefits and risks associated with relevant technology..." [176] Although the recent explosion in Ransomware attacks is a relatively new phenomenon, there is no shortage of resources lawyers can use to become familiar with the threats posed by Ransomware and, consequently, to their clients' data. For example, the FBI has issued guidance that provides "key areas to focus on with Ransomware [such as] prevention, business continuity, and remediation." [177]

P53 With respect to potential regulatory enforcement, the FTC has warned that "a company's failure to update its systems and patch vulnerabilities known to be exploited by Ransomware could violate Section 5 of the FTC Act." [178] In addition, the Gramm-Leach-Bliley Act (GLBA) includes requirements concerning the disclosure by financial institutions of fraudulent access to customer information. [179] The GLBA Safeguards Rule may be used "in conjunction with the FTC's Section 5 authority to bring actions against financial institutions that fail to properly protect consumer financial information." [180] Covered Entities under HIPAA are themselves subject to the Security Rule which, among a myriad of requirements to safeguard patient data, obligates Covered Entities to implement a data backup plan. [181] HIPAA compliance guides indicate that HIPAA security requirements extend to Ransomware, noting "...the possibility of a [R]ansomware attack must now be covered in any risk assessment." [182]

P54 Ransomware attacks also create eDiscovery conundrums. Ransomware as an application has been considered in a number of cases, including with respect to assessing a defendant's behavior to determine whether parole was violated, [183] and in an arbitration regarding the ownership of a domain name. [184] Given the potential for increasingly complex conflicts in this space, practitioners should consider the implications of Ransomware on eDiscovery across a variety of scenarios. These include situations in which Ransomware is the source of a given dispute, as well as when Ransomware becomes a complicating factor in the eDiscovery process. [185]

---

[176] *Comment on Rule 1.1*, AMERICAN BAR ASSOCIATION: THE CENTER FOR PROFESSIONAL RESPONSIBILITY, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html, https://perma.cc/GC6Q-4FN6 (last visited Feb. 12, 2017).

[177] *FBI Internet Crime Complaints*, FLORIDA ATLANTIC UNIVERSITY, http://www.fau.edu/police/images/FBI%20Internet%20Crime%20Complaints.pdf, https://perma.cc/5LLL-JGCE (last visited Feb. 12, 2017);*see also Incidents of Ransomware on the Rise: Protect Yourself and Your Organization, supra* note 168.

[178] Rossen, *supra* note 73.

[179] *See* 15 U.S.C. § 6803; *see also Ransomware - Legal Liability and Enforcement*, FALL 2016 E-NEWSLETTER (Digital Mountain, Santa Clara, C.A.), Oct. 24, 2016, http://digitalmountain.com/enews/FALL_2016_Article3.pdf, https://perma.cc/7YWZ-C3GP.

[180] *Ransomware - Legal Liability and Enforcement, supra* note 179.

[181] *Fact Sheet:* Ransomware and HIPAA, supra note 110.

[182] *Malware Attack, supra* note 76 (quoting John Parmigiani, HIPAA consultant and editorial advisory board member).

[183] *See, e.g.*, United States v. Haymond, No. 08-CR-201-TCK, 2016 WL 4094886, at *2 (N.D. Okla. Aug. 2, 2016).

[184] *See* Virginia College Savings Plan v. Zhouda, 2016 WL 5920046 (UDRP-ARB Dec), at *2-3 (Lowry, Arb.).

[185] *See generally* Ed Silverstein, *Law Firm Among the Latest Victims of Ransomware Attack*, LAW TECHNOLOGY NEWS, Mar. 11, 2015, www.legaltechnews.com/id=1202720266972/Law-Firm-Among-the-Latest-Victims-of-Ransomware-Attack, https://perma.cc/4QVA-3Z4B (detailing a law firm's recent ransomware attack).

P55 Although eDiscovery has not been directly addressed in published decisions that contain a Ransomware element, the duty to preserve remains inviolate. [186] If a matter involves Ransomware, and whether that matter affects the data itself or has secondary implications with respect to the data's unavailability (such as when a hospital is attacked and patients are rerouted to other locations), [187] eDiscovery considerations should be front-of-mind for practitioners. Not only will claims or defenses associated with the Ransomware attack necessarily implicate the technology used, the practices that may have enabled (or failed to prevent) the attack (e.g., the infection vector, the data affected, or the target's backup environment) all may be relevant to the case, thus subject to discovery and requiring preservation.

P56 Yet another potential risk concerns the possibility that Ransomware could negatively impact eDiscovery collection, preservation, and later discovery efforts. The data preserved by eDiscovery collections often includes highly refined sets of important, often "entirely new stores of extraordinarily sensitive information" [188] that are retained for legal hold purposes regardless of the company's standard data retention policies and information governance practices. [189] As discussed above, law firms have become a lucrative target for criminals using Ransomware; [190] among other valuable data sources, information preserved pursuant to litigation holds often is maintained by law firms that are representing multiple companies in a variety of matters. Law firms and other organizations--including vendors that provide preservation-related services--that have custody of these eDiscovery data sets should be cognizant of the risks created by atypical retention practices. These data sets are no less susceptible to Ransomware than their "standard" counterparts--and may even be more attractive targets, given the one-off nature of eDiscovery collections as well as the highly sensitive data they contain. Further, Ransomware may "preserve" data in a sense, but the data cannot be made available for production or may not exist in a usable format, which can add to the eDiscovery conundrums noted above.

IX. RANSOMWARE'S FUTURE

P57 Ransomware appears poised to evolve along the same lines as many other non-criminal programming efforts, increasingly adopting the aesthetic and practicality of popular software instances that rely on a modular design, allowing criminals to "use certain functions as-needed," and offering "much better efficiency" and the "ability to switch tactics as required in the event one method is discovered or is found to be ineffective." [191] This approach would retain certain core elements associated with functional, successful Ransomware variants in play while remaining nimble enough to affect new Internet of Things and mobile device usage.

P58 For example, replacing the usual "command and control" center and related Deep- or Dark-Web business model, future Ransomware might "simply transmit a beacon with a GUID (globally unique identifier) to a Command

---

[186] *See* *Univ. of Montreal Pension Plan v. Bank of Am. Sec., LLC, 685 F. Supp. 2d 456, 462 (S.D.N.Y. 2010).*

[187] *See* Korolov, *supra* note 128.

[188] James A. Sherer, Taylor M. Hoffman & Eugenio E. Ortiz, *Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, e-Discovery, and Information Governance into Due Diligence Practices*, *21 RICH J.L. & TECH 5, P 36 (2015), http://jolt.richmond.edu/v21i2/article5.pdf*, *https://perma.cc/4KBL-2GZ6*.

[189] This is often a mandatory "exception" in many Records and Information Management and Information Governance policies. *See* Vicki Miller Luoma, *Computer Forensics and Electronic Discovery: The New Management Challenge*, 25 COMPUTERS & SECURITY 91, 96 (2006) (When creating an "electronic document retention and deletion policy . . . [a]ny such policy must retain the flexibility to implement litigation holds by suspending routine document deletion" in the face of a reasonable anticipation of litigation).

[190] *See* Crothers, *supra* note 100.

[191] *Ransomware: Past, Present, and Future, supra* note 22.

and Control domain, trying to reach this domain through common protocols/services...to transmit this data." [192] That is, Ransomware applications will be streamlined to suit a market seeking self-service options, exchanging a bespoke process for one that is both easier to replicate on a mass scale and cheaper to produce and distribute. [193]

P59 As noted above, the volume and scope of attacks has expanded as demographics and usage patterns have shifted more and more Ransomware activity onto mobile and Internet of Things devices. [194] In addition, the software and strategy underlying Ransomware attacks has adapted to evade common protective measures; since good backups often are the best defense against serious damage in the event of an attack, newer Ransomware variations have been built to go after those backups as well, destroying "all Shadow Copy and restore point data on Windows systems." [195] Ransomware is being developed to target not only a given piece of hardware, but also the device's local and virtual environment, in an attempt to outwit the efforts of potential victims by guessing at where they might back up their data and undermining those preventative or responsive measures. Future Ransomware may well exploit would-be victims' digital networking or social connections, using information gleaned from online posts to identify additional targets who may value the same types of data and thus be willing to pay the same types of ransoms to secure its release.

P60 Although individuals will no doubt continue to fall victim to Ransomware, the trend seems to be toward attacks carried out on a more ambitious scale. Criminals are said to be "shying away from random attacks," shifting from a focus on individuals and "expanding [further] into the corporate world" where victims are more likely to have the financial wherewithal to pay larger sums. [196] In short, an "individual might be limited to a [US] $ 500 ransom, but how about a manufacturer or a hedge fund?" [197] Criminals can leverage knowledge gained through experience in the ransom marketplace to seek out specific opportunities, determining, for example, that an average person's photos are worth $ X; an investment manager's emails and personal diary are worth $ Y; and a hedge fund's proprietary formulas, representing "need-to-know" intelligence that is jealously guarded, are worth $ Z. Adept attackers have already demonstrated their ability to exploit victim psychology in the abstract; laser-like, focused shakedowns may be the next horizon for Ransomware attacks.

P61 In addition to diversified attack methodology, the potential *impacts* of Ransomware attacks are evolving. Beyond the hijacking or theft of stored financial records or customer files, targeting connected technology has the potential to wreak physical, "real life" havoc. [198] In the case of the Hollywood Presbyterian Medical Center Ransomware attack, for example, in addition to "forcing staff to go back to paper records and fax machines," the

---

[192] *See id.*

[193] Tom Spring, *Dirt Cheap Stampado Ransomware Sells on Dark Web for $ 39*, THREATPOST (July 14, 2016, 12:35 PM), https://threatpost.com/dirt-cheap-stampado-ransomware-sells-on-dark-web-for-39/119284/, https://perma.cc/5FLX-GBPM.

[194] *See* Ben Dickson, *What makes IoT ransomware a different and more dangerous threat*?, TECH CRUNCH, Oct. 2, 2016, https://techcrunch.com/2016/10/02/what-makesiot-ransomware-a-different-and-more-dangerous-threat/, https://perma.cc/8VEP-HUK4.

[195] Korolov, *supra* note 128.

[196] Sutton, *supra* note 127.

[197] *Id.*

[198] *See* Brian Buntz, *The 10 Most Vulnerable IoT Security Targets*, INTERNET OF THINGS INSTITUTE, July 27, 2016, http://www.ioti.com/security/10-most-vulnerable-iot-security-targets?NL=IOT-001UBER&Issue=IOT-001UBER_20160804_IOT-001UBER_796&sfvc4enews=42&cl=article_7&utm_rid=CPG03000004380699&utm_campaign=13637&utm_medium=email&elq2=6a8551b97117440a8d6f316007c6c548, https://perma.cc/8UH5-QPVT.

data loss may have impacted care as "emergency patients were diverted to other hospitals." [199] As we continue to rely more heavily on connected devices, it is not difficult to see how these types of disruptions could create serious problems across multiple industry sectors--the incipient arrival of driverless cars, for example, represents a potentially vulnerable technology that could be exploited for profit by data hostage-takers. An instance of Ransomware may be localized, but its effects can extend much further afield. Cars without accessible data could be paralyzed, regardless of whether they are in motion at the time the attack begins. Picture the movie *Speed*, replacing Sandra Bullock at the helm of a passenger-laden bus with a driverless car heading toward a cliff, doomed to disaster unless a ransom is paid. [200] Likewise, many hospital treatments rely on accurate patient data at critical moments. How much would an individual pay to ensure her blood type is communicated correctly or that his medical history warns doctors of possible drug interactions? If a patient were to die under such circumstances, how would a court assess liability for a failure either to prevent the Ransomware attack, or to pay the ransom promptly?

X. CONCLUSION

> "[Ransomware] is a volume business. It's simple, relatively anonymous and fast. Some people will pay, some will not pay, so what. With a wide enough set of targets there is enough upside for these types of attacks to generate a steady revenue stream." [201]

P62 Grey areas abound, but thoughtful preparation is the best defense; both to avoid a Ransomware attack in the first place, and to manage the issues that may arise when an attack occurs. Practitioners should not only be knowledgeable about Ransomware, which includes understanding Ransomware's operation, effects, and ramifications, but also vigilant in following the latest trends and tracking the ever-evolving threats. Ransomware is not going anywhere, and while the meteoric rise and spread of Ransomware has been startling as a singular issue, it also serves as a clear warning of things to come. There is still plenty of room for innovation and tremendous incentives for criminals to pursue these opportunities. In a marketplace flooded with stolen credit card numbers and digital credentials, selling ill-gotten personal information to identity thieves has become both more cumbersome and less lucrative than holding data hostage and demanding a ransom from its owner. [202]

P63 Given this environment, practitioners should take a proactive approach to understanding Ransomware, not only to counsel clients effectively, but also to safeguard their own sensitive data, both professional and personal. Such understanding demands a working knowledge of digital currencies and ransom payment options, although there is some debate as to whether employing intermediaries [203] may help address that particular challenge. [204] Regardless, the key will be education and vigilance to guide strategic responses to Ransomware incidents. In addition to taking steps to *prevent* Ransomware attacks, practitioners must prepare to *respond* as effectively and efficiently as possible to this ever-evolving threat. [205]

---

[199] Korolov, *supra* note 128.

[200] *See generally* SPEED (Twentieth Century Fox Film Corp. 1994) (a film in which a police officer must drive a bus above 50 miles per hour in order to prevent a bomb from exploding on the bus).

[201] *Raynham Remains Offline in Computer Virus Mystery*, WICKED LOCAL (Mar. 11, 2016, 5:30 PM), http://www.wickedlocal.com/news/20160311/raynham-remains-offline-in-computer-virus-mystery, https://perma.cc/BWW8-J9DF (quoting Brian Contos, ICIT Fellow and VP & Chief Sec. Strategist at Securonix).

[202] *See* Wolff, *supra* note 12.

[203] *See* Sposito, *supra* note 99.

[204] *See* Cutler, *supra* note 158.

[205] *See Practical Steps to Thwart Ransomware and Other Cyberbreaches*, YOUR ABA, Dec. 2016, http://www.americanbar.org/publications/youraba/2016/december-2016/be-prepared-to-thwart-ransomware-and-other-cyber-attacks.html, https://perma.cc/5RX3-WWJG.

Richmond Journal of Law & Technology

Richmond Journal of Law & Technology

End of Document

User Name: Kyle Armstrong
Date and Time: Tuesday, October 17, 2017 5:01:00 PM EDT
Job Number: 55127777

Document (1)

1. *ARTICLE, WHAT SHOULD AN ETHICAL LAWYER KNOW ABOUT TECHNOLOGY?, 46 The Brief 40*

Client/Matter: -None-
Search Terms: ransomware lawyer
Search Type: Natural Language
Narrowed by:

Content Type	Narrowed by
Secondary Materials	-None-

ARTICLE, WHAT SHOULD AN ETHICAL LAWYER KNOW ABOUT TECHNOLOGY?

Winter, 2017

Reporter
46 The Brief 40 *

Author: By J.S. "Chris" Criristie Jr.

J.S. "Chris" Christie Jr.*is a Birmingham, Alabama, partner of Bradley Aram Boult Cummings LLP, where he serves as chair of its Insurance Practice Group and cochair of its Pro Bono Committee. He may be reached at jchristie@bradley.com. Parts of this article were published as "Ethics and Technology," 75 Ala-Law. 31 (2014).*

Text

[*41] Most states recently updated their ethical rules to emphasize a ***lawyer***'s duties to keep up with technology. In light of these updated rules and ever-changing technology, what should an ethical ***lawyer*** know about technology?

Ethical Rules on Technology and Confidentiality

In light of new technology and evolving security concerns, and to guide ***lawyers*** regarding the use of technology, the ABA Model Rules of Professional Conduct were amended in August 2012. [1] The amendments changed Model Rules 1.1 (competence) and 1.6 (confidentiality of information).

Generally, state ethical rules, not the ABA Model Rules, govern ***lawyer*** conduct. Nonetheless, all states except California have adopted a version of the ABA Model Rules, with 31 states as of December 1, 2016, having adopted the 2012 Model Rules technology amendments and another 11 states reporting they are "studying" the amendments. [2] Even for ***lawyers*** in a state that has not adopted these amendments, ethics and technology issues concern every ***lawyer*** practicing today. And ***lawyers*** not adequately addressing technology might find themselves embarrassed, if not worse.

As to Model Rule 1.1, by adding the following phrase beginning with "including" to its comment [8], the 2012 technology amendments stress that competent ***lawyers*** should be aware of basic features of technology: "a ***lawyer*** should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*." Without the amendment to comment [8], a ***lawyer*** already had a duty to keep up with technology; the amendment emphasizes that duty. [3]

---

[1] For background on these ABA Model Rules amendments, see the reports of the ABA Commission on Ethics 20/20, filed May 7, 2012, for the ABA Annual Meeting in August 2012, available at www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html.

[2] *State by State Adoption of Selected Ethics 20/20 Commission Policies, Guidelines for an International Regulatory Information Exchange, and Amendment to Model Rule 8.4*, ABA CENTER FOR PROF. RESP. POL'Y IMPLEMENTATION COMMITTEE, www.americanbar.org/content/dam/aba/administrative/professional_responsibility/state_implementation_selected_e20_20_rules.authcheckdam.pdf (last updated Dec. 1, 2016).

[3] *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 466, at 2 n.3 (Apr. 24, 2014) (discussing whether a ***lawyer***

As to Model Rule 1.6, the amendments add a new paragraph and change two comments. The prior comments already described a ***lawyer***'s ethical duty to take reasonable measures to protect a client's confidential information from inadvertent or unauthorized disclosures, as well as from unauthorized access. In light of the pervasive use of technology to store and send confidential client information, this preexisting obligation is now stated explicitly in the black letter of Model Rule 1.6. The comments were also amended to offer ***lawyers*** more guidance about how to comply with this obligation.

Amended Model Rule 1.6 has the following new paragraph (c): "A ***lawyer*** shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." As examples, a ***lawyer*** should make reasonable efforts to avoid sending a letter or an e-mail to the wrong person, posting confidential client information on social media, or allowing the law firm's computer network to be "hacked."

Comment [16] to Model Rule 1.6, now comment [18], was rewritten to add a list of possible factors to be considered in determining the reasonableness of a ***lawyer***'s efforts to prevent disclosure or access: "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the ***lawyer***'s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)." To comply with Model Rule 1.6(c), instead of risking misdelivery by sending a package by mail, a ***lawyer*** might pay a paralegal to hand deliver the package. But almost all ***lawyers*** would probably agree that such effort is rarely, if ever, required. On the other hand, a ***lawyer*** would want to make sure the mailed package was properly sealed, was correctly addressed, and did not have see-through packaging. Which technology safeguards are comparable to ensuring a package is sealed properly, and which are comparable to hand delivery by a paralegal?

Comment [17] to Model Rule 1.6, now comment [19], has the following new language: "Whether a ***lawyer*** may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules." In other words, ***lawyers*** should also consider duties arising under HIPAA, [4] Gramm-Leach-Bliley (GLB), [5] and other laws intended to protect data privacy.

In light of the Model Rules 2012 technology amendments, what are technology risks in 2017 for ***lawyers***? In addition to computer system security, every ***lawyer*** should consider avoiding scams, password fundamentals, and mobile security. [6]

Computer System Security

---

should research a juror's Internet presence, saying "we are also mindful of the recent addition of Comment [8] to Model Rule 1.1"); Fla. Bar Prof'l Ethics Comm., Op. 10-2 (Sept. 24, 2010) ("If a ***lawyer*** chooses to use these Devices that contain Storage Media, the ***lawyer*** has a duty to keep abreast of changes in technology to the extent that the ***lawyer*** can identify potential threats to maintaining confidentiality.").

[4] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), , and HIPAA's implementing regulations, 45 C.ER. §§ 160-164, regulate the collection, use, and disclosure of medical information by health care providers and their business associates (entities that do business with health care providers; i.e., ***lawyers*** with doctors as clients).

[5] The Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act), *15 U.S.C. §§ 6801-6827*, regulates the collection, use, and disclosure of nonpublic financial information by financial institutions and entities that receive nonpublic financial information from financial institutions (i.e., ***lawyers*** with banks as clients).

[6] The focus here is on legal ethics and the security of confidential information, without attempting to cover all legal ethics issues arising from new technology. For valuable resources on legal ethics relative to other aspects of technology, including social media and metadata, see the ABA Legal Technology Resource Center (LTRC) at *www.americanbar.org/groups/departments_offices/legal_technology_resources/resources.html*.

A hacker can gain computer access by taking advantage of computer systems' vulnerabilities. When identifying parts of a computer system to safeguard, a ***lawyer*** should consider not only servers, desktops, and laptops, but also tablets, smartphones, copiers, scanners, and any other device that can connect to a computer system. A ***lawyer*** should take reasonable steps to make computer systems more secure and to limit the vulnerabilities.

A ***lawyer*** should make sure that his or her computer system has updated antivirus software and other security software, including a firewall. The specifics on programs as safeguards to protect entire computer systems may require a consultant. Unless one is the rare ***lawyer*** with the technical skills, finding someone with expertise to help is advisable.

[*42] A ***lawyer*** should consider regularly updating software and replacing software that is no longer being updated. For example, 10 percent of the ***lawyers*** responding to the ABA's 2015 Legal Technology Survey responded that they still use Windows XP. [7] Windows XP has not been updated or patched since April 2014. [8] Because Microsoft no longer supports Windows XP, it no longer has security updates. Windows XP still operates, but becomes more and more vulnerable to security risks and malware infections as time passes.

According to an *ABA Legal Technology Survey Report* published in September 2014, viruses, spyware, or malware infected nearly half of law firms' computer systems in 2013. Yet, only one-fourth of law firms had any kind of encryption available for their ***lawyers*** to use. [9]

For all electronic data (i.e., information), a ***lawyer*** should consider whether the data should be encrypted. Encryption is the process of encoding data so hackers cannot read it, but authorized parties can. Encryption turns words into scrambled gibberish. Many modern encryption programs use factoring and prime numbers. A prime number can only he divided by one and itself. Factoring is identifying the prime numbers multiplied together that result in a number. Encryption today can make it very difficult for computers to decipher encrypted data without the key.

A ***lawyer*** should consider what data might need to be encrypted. As discussed below, some e-mail programs automatically encrypt data when sent. Another issue is whether to encrypt data at rest. Such encryption complicates the user experience; encrypting all electronic information interferes with using the information efficiently. Data shipped or otherwise taken out of the office creates additional risks. If data relating to the representation of a client is on a portable hard drive, a thumb drive, a mobile device, or attached to an e-mail, whether it should be encrypted requires more thought and depends on a number of factors. Many free encryption tools are available. [10]

A ***lawyer*** should consider whether his or her safeguards are HIPAA and GLB compliant. Even if the ***lawyer*** does not represent health care providers or financial institutions, he or she is likely to have medical and financial information that raises the same or similar confidentiality issues. One might also argue that all confidential information, including attorney-client communications, should be protected with the same or similar safeguards.

A ***lawyer*** should consider regular automatic backups of computer systems. In anticipation of natural disasters, a ***lawyer*** should also consider having such backups in more than one location or at least remote geographically from the main computer systems.

---

[7] David Ries, *Security*, ABA TECHREPORT 2015, *available at*www.americanbar.org/publications/techreport/2015/Security.html.

[8] Catherine Sanders Reach, *Arsenic and Old Lace: Technology Competency*, ADDENDUM (Ala. State Bar), Oct. 2016, *www.alabar.org/assets/uploads/2016/10/Addendum-Oct-2016.pdf*.

[9] Robert Ambrogi, *Viruses Are More Common at Law Firms Than Encryption, ABA Survey Shows*, L. SITES (Sept. 12, 2014), *www.lawsitesblog.com/2014/09/viruses-much-common-law-firms-encryption-aba-survey-shows.html*.

[10] Casper Manes, *The Top 24 Free Tools for Data Encryption*, GFI TALK (June 12, 2015), *www.gfi.com/blog/the-top-24-free-tools-for-data-encryption/*.

A ***lawyer*** should consider the risks a vendor (third-party service provider) presents to data security. "Vendors are consistently cited as a primary cause of data breaches." [11] Just like other businesses, a ***lawyer*** should exercise reasonable due diligence selecting vendors, have contracts with vendors requiring them to safeguard data, and monitor vendors to confirm that they are complying.

Another issue involves the cloud, which has nothing to do with weather. Years ago, when engineers were diagramming computer networks, they did not know how to represent the Internet, so they just drew a cloud. Today, "the cloud" means a computer accessible through the Internet. If a ***lawyer*** is using the cloud, the ***lawyer*** stores data on a computer owned by a third party. Because cloud computing places client data on remote servers not in a ***lawyer***'s direct control, an issue is whether ***lawyers*** can use the cloud.

Twenty states have considered the issue and advised that ***lawyers*** can use cloud computing, if they exercise reasonable care. [12] Often, using a cloud vendor is more secure than what a ***lawyer*** might be able to have on the ***lawyer***'s own computer systems. A cloud vendor is also likely to have better backup capability. If considering a cloud vendor, a ***lawyer*** might ask or investigate the following questions:

[*43] - How does the vendor safeguard data?
- Are the vendor's safeguards HIPAA and GLB compliant?
- After data is deleted, can the vendor certify that it is destroyed?
- How often does the vendor back up data?
- Does the vendor back up data in multiple locations?
- How stable is the vendor as a business entity?
- Does accessing the ***lawyer***'s data require proprietary software?
- If the relationship ends, how is the data accessed and returned?
- What confidentiality provisions are in the vendor's standard contract?
- Will the vendor agree to other confidentiality provisions?

In summary, when choosing a cloud vendor, a ***lawyer*** should consider whether the data will be secure and backed up and whether the ***lawyer*** will have any problems if and when his or her relationship with the vendor might end.

Examples of cloud storage and sharing services include Dropbox, Google Drive, Box, and Microsoft OneDrive for Business. [13] Dropbox is the most popular cloud file storage and sharing service, with more than 300 million users, including many ***lawyers***. Whether Dropbox, even Dropbox for Business, is secure enough for businesses has been questioned. [14] In 2016, Dropbox apparently responded to these concerns, publishing "Dropbox Business Security:

---

[11] John Thomas A. Malatesta III & Sarah S. Glover, *A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses*, 17 SEDONA CONF. J. 761 (2016). For any business considering data security, this article has numerous action items and considerations when evaluating existing or potential vendors.

[12] *See Cloud Ethics Opinions around the U.S.*, ABA LTRC, www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited Jan. 5, 2017).

[13] *Dropbox Alternatives: 10 Best Cloud Storage Services*, BEEBOM, http://beebom.com/best-dropbox-alternatives-for-cloud-storage/ (last updated Mar. 1, 2016).

[14] Mike Batters, *Security Comment: Why Are People Still Using Dropbox for Business?*, LEGAL IT INSIDER (Apr. 14, 2016), www.legaltechnology.com/latest-news/security-comment-why-are-people-still-using-dropbox-for-business/.

A Dropbox Whitepaper." [15] For whatever reasons, Dropbox has been identified annually since 2013 as the app that companies ban more than any other app. [16]

A final computer system consideration might be what to do with computers when they are no longer being used. ***Lawyers*** should be careful when discarding computers, copiers, and any other devices storing data. A possible risk that might be missed is data on leased computers and copiers. Note that Affinity Health Plan Inc. paid a fine of $ 1,215,780 for alleged HIPAA violations after it returned multiple copiers to a leasing agent without erasing data on the copiers' hard drives. [17]

Avoiding Scams

Avoiding scams sounds almost too obvious to include as something ***lawyers*** should consider. Nonetheless, when people say their computer has been hacked, they probably mean the hacker deceived someone into allowing direct access to the computer or into sharing a password. A ***lawyer*** should learn how to detect and to avoid such scams and should train his or her staff on how to detect and to avoid scams.

Because secure computer systems are difficult to access from outside, hackers often attempt to gain access by deceiving someone. Generally, hackers use two deceptive methods: (1) sending phishing and spoofing e-mails, which urge the e-mail recipient to respond; or (2) using malware that a recipient downloads with games or other apps or by opening infected e-mail attachments, infected thumb drives, or unsafe websites that infect a computer visiting it.

With a phishing e-mail, the sender is fishing for information to use for whatever purposes the sender can imagine. Spoofing is creating a deceptive e-mail that looks like it is sent by a legitimate business--for example, a hank. Many phishing e-mails spoof a specific business's e-mails, often with an e-mail address that looks like the spoofed business's e-mail address.

If a cursor is hovered over (do not click) an e-mail sender's name, the sender's e-mail address and its domain name is shown. For an e-mail with links, if a cursor is **[*44]** hovered over (do not click) the link, the link's Internet website address (Uniform Resource Locator, or URL) is shown. The domain name or the URL should match what one expects. A creative spoofing e-mail might have names that are close to those being spoofed, but with slight differences; for example, "bradlley" with two *l*s, rather than "bradley" with one *l*. If an e-mail's sender's domain names or link URLs make one suspicious, the e-mail is probably a phishing e-mail.

Malware is short for malicious software. It includes computer viruses, worms, Trojan horses, ***ransomware***, spyware, and other malicious programs.

An infamous malware example is the Melissa virus, which first appeared in 1999. [18] E-mails with an attachment spread this computer virus. After a Melissa virus e-mail recipient opens the attachment, the virus replicates itself by creating e-mails with the same attachment and sending them to the first 50 addresses in the recipient's Outlook address book. Unless contained, the Melissa virus can shut down e-mail systems with the huge number of e-mails.

---

[15] *Available at*https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vflDw-Ksl.pdf.

[16] James Bourne, *MobileIron Security Report: iOS Increases Dominance, Dropbox Most Banned Consumer App*, ENTERPRISE APPSTECH (Aug. 2, 2016), www.appstechnews.com/news/2016/aug/02/mobileiron-security-report-ios-increases-dominance-dropbox-most-banned-consumer-app/.

[17] *HHS Settles with Health Plan in Photocopier Breach Case*, HHS.GOV, www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/health-plan-photocopier-breach-case/index.html (last visited Jan. 5, 2017).

[18] *See* Jonathan Strickland, 10 *Worst Computer Viruses of All Time*, HOWSTUFFWORKS TECH (Aug. 26, 2008), http://computer.howstuff-works.com/worst-computer-viruses1.htm.

Today, probably the most serious malware risk is ***ransomware***. [19] ***Ransomware*** stops one from normally using an infected computer and requires doing something before normal computer use returns. Usually, ***ransomware*** requires paying money (a "ransom") to the hacker. [20] ***Ransomware*** can encrypt files making them unusable, prevent access to Windows, or stop certain apps from working.

In 2016, ***ransomware*** attacks in the United States averaged 4,000 per day, costing over $ 200 million in the first three months of 2016. [21] For example, in February 2016, Hollywood Presbyterian Medical Center paid a $ 17,000 ransom in bitcoin to a hacker who seized control of the hospital's computer systems. [22] A September 2016 article reported that two-thirds of ***ransomware***-infected companies in the United Kingdom pay ***ransomware*** demands, but not all get their data back. [23]

When considering safeguards to protect against malware, the types of computers at risk include servers, desktops, laptops, tablets, smartphones, and any other device that can download data or access the Internet. ***Lawyers*** should be able to reduce malware risks, [24] including ***ransomware*** risks, with the following steps:

- Do not open risky e-mails or e-mail attachments;
- Do not click on risky links in e-mails or websites;
- Do not download games or nonwork apps;
- Do not open risky thumb drives or CDs;
- Do not visit unsafe, suspicious, or fake websites;
- Block unsafe, suspicious, or fake websites;
- Install up-to-date antivirus and security software;
- Update software, replacing if no longer updated;
- Separate work and personal computer use; [25] and
- Backup important files in a remote, unconnected facility.

Lawyers have recently been targets of scams, including one based on phishing e-mails with a link to view a business complaint that opens a website that installs ***ransomware***. [26] In the first quarter of 2016, PhishMe reported

---

[19] *See* ***Ransomware***, MICROSOFT MALWARE PROTECTION CENTER, *www.microsoft.com/en-us/security/portal/mmpc/shared/**ransomware**.aspx* (last visited Jan. 5, 2017).

[20] For example, a Pennsylvania district attorney's office recently paid about $ 1,400 in bitcoin to a malware ring known as the Avalanche. Joe Mandak, *Prosecutor's Office Paid Bitcoin Ransom in Cyberattack*, ABC NEWS (Dec. 5, 2016), *http://abcnews.go.com/Technology/wireStory/feds-business-lost-387500-world-cybercrime-operation-43985864*.

[21] Rebecca Campbell, FBI *Now Says Don't Pay Bitcoin to* ***Ransomware*** *Extortionists*, CRYPTOCOINS NEWS (Aug. 9, 2016), *www.cryptocoinsnews.com/fbi-now-says-dont-pay-bitcoin-**ransomware**-extortionists/*.

[22] Richard Winton, *$ 17,000 Bitcoin Ransom Paid by Hospital to Hackers Sparks Outrage*, L.A. TIMES, Feb. 19, 2016, *www.latimes.com/business/technology/la-me-In-17000-bitcoin-ransom-hospital-outrage-20160219-story.html*.

[23] Danny Palmer, *Two-Thirds of Companies Pay* ***Ransomware*** *Demands: But Not Everyone Gets Their Data Back*, ZDNET (Sept. 7, 2016), *www.zdnet.com/article/two-thirds-of-companies-pay-**ransomware**-demands-but-not-everyone-gets-their-data-back/*.

[24] *See Help Prevent Malware Infection OR Your PC*, MICROSOFT MALWARE PROTECTION CENTER, *www.microsoft.com/en-us/security/portal/mmpc/shared/prevention.aspx* (last visited Jan. 5, 2017).

[25] If separate computers are not possible, at least have separate accounts on the same computer (especially if a child is using it).

[26] Debra Cassens Weiss, *Don't Click!* ***Lawyers*** *Get Fake Emails about a Complaint; Hyperlink Installs Malicious Software*, A.B.A. J. (Dec. 5, 2016),

that 93 percent of phishing e-mails were related to ***ransomware***. [27] What are red flags indicating that an e-mail is risky?

- Asks for login and password;
- Purports to be from the IRS, a court, or other government entity;
- Purports to be from a financial institution or health care provider;
- Requests personal information like account numbers;
- Has suspicious or misspelled sender e-mail address or domain;
- Has links with suspicious URL addresses;
- Requests clicking on unfamiliar links;
- Has generic, unusual, or incorrect name in greeting;
- Makes an urgent request with a short deadline like 24 hours; or
- Requests to download a file, especially an .exe file.

The red flag of an e-mail's asking for login and password information should be the most obvious one. Providing another with one's login and password is always very risky, but replying to an e-mail with that information is bad--but people must do it, because phishing e-mails keep asking for that information.

Most of the above red flags can apply to considering whether a link, website, or social media post is risky. Common sense can help too.

Some e-mail scams are even more sophisticated. "Social engineering" refers to psychologically manipulating people into performing actions or disclosing confidential information. [28] Victims are often motivated by wanting to help. In this context, social engineering might entail the hacker learning enough about a law firm to pose as the managing partner and send a "spear phishing" e-mail to the firm's controller. Avoiding sophisticated scams may require slowing down, research, and common sense before action.

A ***lawyer*** should consider having a technology risks training program for all who have access, through the ***lawyer***'s computer systems, to the Internet or to e-mails. While a cliché, a chain is only as strong as its weakest link. A hacker usually has as much access to a ***lawyer***'s

End of Document

www.abajournal.corri/news/article/dont_click_***lawyers***_get_fake_emails_about_a_complaint_hyperlink_installs_mal/?utm_source=internal&utm_medium=navigation&utm_campaign=most_read.

[27] *Q1 2016 Sees 93% of Phishing Emails Contain* ***Ransomware***, PHISHME (June 4, 2016), *http://phishme.com/q1-2016-sees-93-phishing-emails-contain-**ransomware**/*.

[28] *What Is Social Engineering?*, WEBROOT, *www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering* (last visited Jan. 5, 2017).

Data protection in the United States: overview

by *Ieuan Jolly*, Loeb & Loeb

Law stated as at 01 Jul 2017 • USA (National/Federal)

A Q&A guide to data protection in the United States.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the data protection Country Q&A tool.

This article is part of the global guide to data protection. For a full list of contents, please visit www.practicallaw.com/dataprotection-guide.

Contents

Regulation

Legislation

1. What national laws regulate the collection and use of personal data?

General laws
Not applicable.

Sectoral laws

In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. However, each Congressional term brings proposals to standardise laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices". These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators.

There are already a panoply of federal privacy-related laws that regulate the collection and use of personal data. Some apply to particular categories of information, such as financial or health information, or electronic communications. Others apply to activities that use personal information, such as telemarketing and commercial e-mail. In addition, there are broad consumer protection laws that are not privacy laws per se, but have been used to prohibit unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information.

Some of the most prominent federal privacy laws include, without limitation, the following:

- The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorised disclosure of personal data. The FTC is also the primary enforcer of the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506), which applies to the online collection of information from children, and the Self-Regulatory Principles for Behavioural Advertising.
- The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) regulates the collection, use and disclosure of financial information. It can apply broadly to financial institutions such as banks, securities firms and insurance companies, and to other businesses that provide financial services and products. GLB limits the disclosure of non-public personal information, and in some cases requires financial institutions to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared. In addition, there are several Privacy Rules promulgated by national banking agencies and the Safeguards Rule, Disposal Rule, and Red Flags Rule issued by the FTC that relate to the protection and disposal of financial data.
- The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) regulates medical information. It can apply broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information. The Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (45 C.F.R. Parts 160 and 164) apply to the collection and use of protected health information (PHI). The Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule) (45 C.F.R. 160 and 164) provides standards for protecting medical data. The Standards for Electronic Transactions (HIPAA Transactions Rule) (45 C.F.R. 160 and 162) applies to the electronic transmission of medical data. These HIPAA rules were revised in early 2013 under the HIPAA “Omnibus Rule”.
- The HIPAA Omnibus Rule also revised the Security Breach Notification Rule (45 C.F.R. Part 164) which requires covered entities to provide notice of a breach of protected health information. Under the revised rule, a covered entity must provide notice of acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, unless the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised.
- The Fair Credit Reporting Act (15 U.S.C. §1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) which amended the Fair Credit Reporting Act) applies to consumer reporting agencies, those who use consumer reports (such as a lender) and those who provide consumer-reporting information (such as a

credit card company). Consumer reports are any communication issued by a consumer reporting agency that relates to a consumer's creditworthiness, credit history, credit capacity, character, and general reputation that is used to evaluate a consumer's eligibility for credit or insurance.

- The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) and the Telephone Consumer Protection Act (47 U.S.C. §227 et seq.) regulate the collection and use of e-mail addresses and telephone numbers, respectively.
- The Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030) regulate the interception of electronic communications and computer tampering, respectively. A class action complaint filed in late 2008 alleged that internet service providers (ISPs) and a targeted advertising company violated these statutes by intercepting data sent between individuals' computers and ISP servers (known as deep packet inspection). This is the same practice engaged in by Phorm in the UK and several UK telecommunications companies that resulted in an investigation by the European Commission.
- In 2016, Congress enacted the Judicial Redress Act, giving citizens of certain ally nations (notably, EU member states) the right to seek redress in US courts for privacy violations when their personal information is shared with law enforcement agencies.
- On 3 April 2017, President Donald Trump signed into law a bill that repealed a set of privacy and data security regulations for broadband internet service providers adopted by the Federal Communications Commission (FCC) in the last months of the Obama administration. The FCC adopted the Privacy Rule for broadband ISPs at the end of October 2016, after acknowledging that "the current federal privacy regime, including the important leadership of the Federal Trade Commission (FTC) and the Administration efforts to protect consumer privacy, does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks." The FCC Privacy Rule (which would have taken effect later in 2017) established a framework of customer consent required for ISPs to use and share their customers' personal information that was calibrated to the sensitivity of the information. The rules would have incorporated the controversial inclusion of browsing history and apps usage as sensitive information, requiring opt-in consent. They also would have included data security and breach notification requirements. The Federal Trade Commission (FTC), which oversees consumer privacy compliance for other companies, does not currently treat consumer browsing history or apps usage as sensitive data.

Other laws and guidelines

There are also many federal security and law enforcement laws that regulate the use of personal information, but these laws are outside the scope of this chapter.

In addition to the above laws, there are also many guidelines issued by industry groups that are not legally enforceable but are generally considered "best practices" in those industries (such as the payment card, mobile marketing and online advertising industries). For example, the advertising industry continues to develop its self-regulatory programme for online behavioural advertising. This programme requires members of various advertising industry trade groups to comply with the groups' guidelines for online behavioural advertising, which largely mirror the FTC's guidelines .The programme includes an icon that members should place on their websites if tracking data is collected. The icon links to information about the website's data collection practices and how an individual can opt out of some online tracking. The self-regulatory programme was also expanded in 2015 to the mobile environment.

State privacy laws

There are many laws at the state level that regulate the collection and use of personal data, and the number grows each year. Some federal privacy laws pre-empt state privacy laws on the same topic. For example, the federal law regulating commercial e-mail and the sharing of e-mail addresses pre-empts most state laws regulating the same

activities. Conversely, there are many federal privacy laws that do not pre-empt state laws, which means that a company can find itself in the position of trying to comply with federal and state privacy laws that regulate the same types of data (for example, medical or health records) or types of activity.

Most states have enacted some form of privacy legislation, however California leads the way in the privacy arena, having enacted multiple privacy laws, some of which have far-reaching effects at a national level.

California was the first state to enact a security breach notification law (California Civil Code §1798.82). The law requires any person or business that owns or licenses computerised data that includes personal information to disclose any breach of the security of the system to all California residents whose unencrypted personal information was acquired by an unauthorised person.

Most of the early state security breach notification laws mirrored California's law, and tended to be reactive, that is, they established requirements for responding to a security breach. More recently, a number of states laws have enacted more prescriptive and preventative laws, that is, these laws are more stringent and actually establish requirements to avoid a security breach. The best example of a preventative-type of law is the Massachusetts Regulation (201 CMR 17.00), which prescribes in considerable detail an extensive list of technical, physical and administrative security protocols aimed at protecting personal information that affected companies must implement into their security architecture, and describe in a comprehensive written information security programme.

As of April 2017, 48 states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands all have enacted laws requiring notification of security breaches involving personal information. Alabama and South Dakota are the only states with no security breach law.

New laws and proposed amendments are constantly proliferating, as technological threats change and progress toward uniform federal legislation stalls. For example, California is seeing the implementation of a variety of data privacy laws and amendments it enacted in 2015 including:

- The California Electronic Communications Privacy Act (S.B. 178), which severely limits the ability of government authorities to seek electronic communication information for law enforcement purposes.
- Several amendments to security breach notification law. S.B. 570 amends the required content of security breach notices, requiring that notices clearly and conspicuously display certain prescribed headings. A.B. 964 now defines the term "encrypted" for purposes of California's breach notification law as "rendered unusable, unreadable, or indecipherable to an unauthorised person through a security technology or methodology generally accepted in the field of information security." Both amendments went into effect on 1 January 2016.
- A.B. 1541, which amends the definition of "personal information" in the state's data privacy statute to include:
  - a username or e-mail address combined with a password or security question and answer for access to an online account; and
  - health insurance information.

Scope of legislation

2. To whom do the laws apply?

The FTC Act. This applies to most companies and individuals doing business in the US, other than certain transportation, telecommunications and financial companies (because these industries are primarily regulated by other national agencies). The FTC's Behavioural Advertising Principles are voluntary in nature, although many companies consider them "best practices". They apply to website operators that engage in behavioural advertising (contextual advertising and targeted advertising).

The GLB Act. This applies to financial institutions, defined to include a range of institutions engaging in financial activities, such as banks, securities firms and insurance companies. According to the FTC, the primary enforcer of GLB, an institution must be significantly engaged in financial activities to be considered a financial institution. Whether a financial institution is significantly engaged in financial activities to come under GLB. Whether an institution is significantly engaged in financial activities is a flexible standard that takes into account all the facts and circumstances.

GLB also applies to third parties that are not financial institutions but that receive non-public personal information from non-affiliated financial institutions.

The HIPAA. This applies to covered entities and business associates. Covered entities include health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. These activities include:

- Claims processing or administration.
- Data analysis and processing.
- Quality assurance.
- Billing.
- Benefit management.
- Practice management.
- Re-pricing.

The California Security Breach Notification Law. This applies to any person or business that conducts business in California and that owns or licenses computerised data that includes personal information.

The California Online Privacy Protection Act. This applies to an operator of a commercial website, online service or mobile app, that collects personally identifiable information through the internet about individual consumers residing in California who use or visit its commercial website or online service.

3. What data is regulated?

The FTC Act does not regulate specific categories of data. Instead it prohibits unfair or deceptive acts or practices involving practices that fail to safeguard consumers' personal information. The FTC's Behavioural Advertising Principles apply to the tracking of a consumer's activities online over time, including the consumer's searches, web pages visits, and viewed content, to deliver advertising targeted to the individual consumer's interests.

The GLB Act applies to non-public personal information collected by a financial institution that is provided by, results from, or is otherwise obtained in connection with consumers and customers who obtain financial products or services primarily for personal, family or household purposes from a financial institution.

For the purposes of the GLB Act, a consumer is someone who has obtained a financial product or service but does not have an ongoing relationship with the financial institution (for example, someone who cashed a check with a check-cashing company or made a wire transfer or applied for a loan). A customer is a sub-set of consumers and refers to someone with an ongoing relationship with the institution. The non-public personal information that is the subject of GLB applies to information that is not publicly available and which is capable of personally identifying a consumer or customer.

The HIPAA regulates PHI, which is individually identifiable health and medical information that is maintained or transmitted by a covered entity or its business associate.

The California Security Breach Notification Law regulates personal information, which means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number.
- Driver's licence number or California Identification Card number.
- Account number, credit or debit card number, in combination with any required security code, access code or password that allows access to an individual's financial account.
- Medical information.
- Health insurance information.

Personal information also includes a user name or email address, in combination with a password or security question and answer that would permit access to an online account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

The California Online Privacy Protection Act defines personally identifiable information as individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

- A first and last name.
- A home or other physical address, including street name and name of a city or town.
- An e-mail address.
- A telephone number.
- A social security number.
- Any other identifier that allows the physical or online contacting of a specific individual.

Information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described above.

4. What acts are regulated?

The FTC Act prohibits unfair or deceptive acts or practices. The FTC has used its authority to charge companies that:

- Fail to protect consumer personal data, leaving such data vulnerable to cyberattacks.
- Have changed their privacy policies without adequate notice.
- Fail to comply with a posted privacy policy.

The GLB Act regulates the collection, use, sharing and disclosure of non-public financial information. The requirements for written notice of privacy procedures and obtaining consent (and opportunities to opt-out of certain disclosures) vary depending on whether the data subject is a customer or a consumer and with whom the financial institution shares this information. One of the most onerous obligations financial institutions is to implement a security programme to protect the non-public personal information from unauthorised disclosures.

The HIPAA regulates the use and disclosure of PHI and the collection, use, maintenance or transmission of electronic PHI, and requires notice of privacy practices.

The California Security Breach Notification Law requires any person or business that conducts business in California and owns or licenses computerised data that includes personal information to disclose any security breach of this information following discovery or notification of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person. In addition, any person or business that maintains computerised data that includes personal information that the person or business does not own must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorised person. If the person or business providing the notification was the source of the breach, an offer

to provide appropriate identity theft prevention and mitigation services, if any, must be provided at no cost to the affected person for not less than 12 months.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes its information handling procedures. As amended, the Act requires operators of web sites, online services and mobile apps that are directed to minors or that have actual knowledge that a minor is using their site or service to both:

- Permit a minor to remove or request the removal of certain online information.
- Disclose how minors can remove or request removal of content.

The Act also prohibits such operators from advertising and marketing products not legally available to minors (including alcohol, firearms, tobacco, tattoos and lottery tickets).

5. What is the jurisdictional scope of the rules?

The FTC Act and rules and guidelines promulgated under the FTC's authority apply to companies and individuals doing business in the US.

The GLB Act applies to financial institutions (which is defined very broadly, see *Question 2*) and to affiliated and non-affiliated third parties that receive non-public personal information from financial institutions. It also applies to persons who obtain or attempt to obtain, or cause or attempt to cause disclosure of, that non-public personal information from financial institutions through false or fraudulent means.

The HIPAA covers entities (defined in *Question 2*) over which the US Government has enforcement authority. However, certain business associates of covered entities may have contractual obligations to safeguard PHI, including those operating outside of any US jurisdiction.

The California Security Breach Notification Law applies to any person or business that conducts business in California, and that owns or licenses computerised data that includes personal information.

The California Online Privacy Protection Act applies to an operator of a commercial website or online service that collects personally identifiable information through the internet about individual consumers residing in California who use or visit its commercial website or online service.

6. What are the main exemptions (if any)?

The privacy rules and guidelines issued by the FTC provide exemptions from privacy requirements for law enforcement purposes.

Under the GLB Act, a financial institution can disclose a consumer's non-public personal information with an affiliated entity if it provides notice of this practice. The financial institution does not need to obtain consent for this disclosure. An affiliated entity is any company that controls, or is controlled by, or is under common control with another company, including financial and non-financial institutions.

A financial institution can disclose a consumer's non-public personal information with a non-affiliated entity without providing the consumer the right to opt out if all the following apply:

- The disclosure is to a third party that uses the information to perform services for the financial institution.
- The financial institution provides notice of this practice.
- The financial institution and the third party enter into a contract that requires the third party to maintain the confidentiality of the information and to use the information only as intended.

A financial institution can disclose a consumer's non-public personal information with a non-affiliated entity without providing the consumer the right to opt out if the information is necessary to effect, administer or enforce a transaction. In this case, the financial institution does not need to disclose this practice to the consumer.

A financial institution can disclose non-public personal information for compliance purposes (for example, to an insurance rating organisation) and for law enforcement purposes. A financial institution can disclose publicly available financial information (such as publicly available property tax records).

The HIPAA does not apply to health information that is not personally identifiable (for example, aggregate data), and it does not apply to health information used by individuals or entities that do not fall within the definitions of covered entities or business associates of covered entities. For example, some educational and employment records (such as a report about an individual's fitness for duty used to make an employment decision) does not fall under HIPAA. There are many exemptions from the restrictions on disclosure of PHI, for example, for law enforcement purposes and to avert a serious public health threat.

The disclosure of a security breach required by the California Security Breach Notification Law may be delayed if a law enforcement agency determines the notification will impede a criminal investigation. In addition, a company that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the law, is deemed to comply with the notification requirements if the person or business notifies subject persons in accordance with its policies if there is a breach of the system's security.

For California Online Privacy Protection Act requirements, see *Question 4*.

Notification

7. Is notification or registration required before processing data?

The FTC's Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to online behavioural advertising and disclose that consumers can opt out of these practices, providing an opt-out mechanism.

The GLB Act requires a financial institution to provide notice of its privacy practices, but does not have the same government regulator notification or registration requirements under Directive 95/46/EC on data protection (Data Protection Directive).

The HIPAA requires a covered entity to provide notice to data subjects of its privacy practices and of data subjects' rights under HIPAA, but does not have the same government regulator notification or registration requirements as under the Data Protection Directive.

The California Security Breach Notification Law does not have the same government regulator notification or registration requirements as under the Data Protection Directive. However, if a security breach occurs, notice should be provided in certain circumstances to all affected individuals in one of the following forms:

- Written notice.
- Electronic notice, if the notice provided is consistent with national laws concerning electronic signatures (*15 U.S.C. §7001*).
- Substitute notice, if the company demonstrates that the cost of providing notice would exceed US$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the company does not have sufficient contact information.

Substitute notice must consist of all of the following:

- E-mail notice when the company has an e-mail address for the subject persons.
- Conspicuous posting of the notice on the agency's website page, if the agency maintains one.
- Notification to major state-wide media.

However, if a company maintains its own notification procedures through an information security policy for personal information and is otherwise consistent with legal timing requirements, the company complies with the notification requirements if it notifies subject persons in accordance with its policies if there is a breach of system security. Companies must submit to the California Attorney General a copy of the notification that was sent to affected consumers.

The California Online Privacy Protection Act requires commercial websites to disclose their privacy practices, but does not have the same government regulator notification or registration requirements under the Data Protection Directive.

Main data protection rules and principles

Main obligations and processing requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The FTC has used section 5 of the FTC Act to charge companies that failed to comply with their own privacy policies or failed to safeguard data they have collected. The FTC Act does not expressly require a company to have or disclose a privacy policy, but the FTC's position is that if a company discloses a privacy policy, it must comply with it. In addition, the FTC has stated that it is a violation of the FTC Act for a company to retroactively change its privacy policy without providing data subjects an opportunity to opt out of the new privacy practice.

In 2015-17, the FTC:

- Levied a US$100 million penalty against LifeLock, after Lifelock violated a 2010 order and failed to secure customer's personal data. This is the largest monetary penalty the agency has ever levied in an order-enforcement action.
- Won a notable appellate victory, with the Third Circuit affirming the Commission's authority to prosecute unreasonable data security practices under section 5 of the FTC Act. The defendant hotel chain ultimately settled with the FTC, but the appellate decision was significant in ruling that the FTC could use its general consumer protection authority to crack down on inadequate security measures as unfair and deceptive and practices.
- Released guidance to help companies take the appropriate actions in the wake of a data breach, in response to reports that data breaches at numerous companies put sensitive personal information belonging to hundreds of millions of consumers at risk.
- Ensured compliance with the (now-defunct) EU-U.S. Safe Harbour framework. For example, the FTC entered settlements with 13 companies over charges that they falsely represented compliance with their self-certification requirements under Safe Harbour rules.

Some bills advanced or introduced in the 115th Congressional term (Jan. 2017 – Jan. 2018) include:

- H.R. 387 (Email Privacy Act). This amends title 18, US Code to update the privacy protections for electronic communications information that is stored by third-party service providers to protect consumer privacy interests while meeting law enforcement needs and for other purposes (introduced on 9 January 2017, passed by House on 6 Feb 2017).
- H.R. 2454 (Department of Homeland Security Data Framework Act of 2017). This directs the Secretary of Homeland Security to establish a data framework to provide access for appropriate personnel to law enforcement and other information of the Department, and for other purposes (introduced on 16 May 2017).
- H.R. 2356 (Managing Your Data Against Telecom Abuses Act of 2017, or the MY DATA Act of 2017). This prohibits providers of internet broadband services or of internet content, applications, or devices from using unfair, or deceptive acts or practices relating to privacy or data security. The Federal Trade Commission (FTC), , can promulgate regulations to carry out such prohibition after consulting with the Federal Communications Commission (FCC). (Introduced on 4 May 2017 and a similar bill, S. 984, was introduced in the Senate on 27 April 2017).
- H.R. 2520 (Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, or the "BROWSER Act"). This requires providers of broadband internet access service and edge services to:
- clearly notify users of their privacy policies; and
- give users opt-in or opt-out approval rights with respect to the use of, disclosure of, and access to user information collected by the providers based on the level of sensitivity of the information, and for other purposes (introduced on 18 May 2017).

The GLB Act seeks to protect consumer financial privacy by limiting when a financial institution can disclose a consumer's non-public personal information to non-affiliated third parties. Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to opt out if they don't want their information shared with certain non-affiliated third parties. (See *Question 3* for definitions of customer and consumer.) Another part of GLB is the Safeguards Rule, which requires companies to develop a written information security plan that describes their programme to protect customer records and information. Federal and state agencies with jurisdiction under GLB over financial institutions must implement regulations requiring the financial institutions to establish safeguards under their security programme, including safeguards that:

- Protect against unauthorised access to, or use of, these records or information, which would result in substantial harm or inconvenience to any customer. Common standards that have been suggested to restrict unauthorised access include the use of:
  - data encryption;
  - authentication mechanisms;
  - background checks; and
  - frequent monitoring and testing of the information security protocols and systems.
- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of these records.
- Implement an identity theft prevention programme in connection with covered accounts.
- Implement response programme regulations requiring the financial institutions to notify the regulator (and in certain cases the customer) when there has been unauthorised access to sensitive customer information.
- Contractually require its service providers to ensure that they are also meeting the objectives of the security programme and monitor them.

In addition, any entity that receives consumer financial information from a financial institution can be restricted in its reuse and re-disclosure of that information.

The HIPAA requires (with some exceptions) covered entities to:

- Use, request and disclose the minimum amount of PHI necessary to complete a transaction (*HIPAA Privacy Rule*).
- Implement data security procedures, protocols and polices at administrative, technical, physical and organisational levels to protect data (*HIPAA Security Rule*).
- Comply with certain uniform standards established for certain electronic transactions (*HIPAA Transactions Rule*).

The California Security Breach Notification Law is triggered by unauthorised disclosure of unencrypted information, so it encourages companies to encrypt the personal information of Californians. An amendment enacted in 2015 defined encryption under the law, without specifying technological standards. Another California statute, Civil Code §1798.81.5, requires certain businesses to use safeguards to ensure the security of Californians' personal information (defined as name plus social security number, driver's licence or state ID and financial account number) and to contractually require third parties to do the same. Civil Code §§1798.85-1798.86, 1785.11.1, and 1785.11.6 restrict businesses and state and local agencies from publicly posting, displaying selling or offering to sell social security numbers and prohibit embedding social security numbers on a card or document using a bar code, chip, magnetic strip or other technology, in place of removing the number as required by law. Civil Code §§1798.80 to 1798.81 and 1798.84 require businesses to shred, erase or otherwise modify the personal information in records under their control.

For California Online Privacy Protection Act requirements, see *Question 4*. For the requirements for these privacy policies, see *Question 12*.

9. Is the consent of data subjects required before processing personal data?

The FTC's Behavioural Advertising Principles suggest website operators should obtain affirmative express consent (which can be provided online) before using sensitive consumer data. Sensitive data includes:

- Financial data.
- Data about children.
- Health information.
- Precise geographic location information.
- Social security numbers.

In addition, website operators that revise their privacy policies should obtain affirmative express consent before using consumer data in ways that are materially different from the privacy policy that was in effect when the data was collected. The FTC also enforces the Children's Online Privacy Protection Act which requires websites that are

directed to children, or that knowingly collect personal information from children, to obtain verifiable parental consent before sharing children's personal information.

The GLB Act requires a financial institution, at the time of establishing a customer relationship, and at least annually after that, to notify customers and consumers of the institution's privacy policy and practices and allow the individual to opt-out of certain disclosures of the individual's non-public personal information. A financial institution must provide the consumer or customer with reasonable means to opt-out of certain disclosures (such means can be written, oral or electronic).

The HIPAA generally requires covered entities to obtain consent in writing from a data subject before disclosing that data (with certain exceptions, for example, to provide medical treatment). Consent must generally be in writing and contain the signature of the data subject and the date. The HIPAA Privacy Rule provides specific statements that must be included in the consent.

The California Security Breach Notification Law requires disclosure of security breaches, but does not specifically address the requirement for consent. However, other California statutes require express consent when processing personal information, for example, California's medical privacy law (*Civil Code §1798.91*) prohibits using personal medical information for direct marketing purposes without consent.

For California Online Privacy Protection Act requirements, see *Question 4*, but these do not specifically address the requirement for consent.

10. If consent is not given, on what other grounds (if any) can processing be justified?

The FTC Act does not specifically address consent (see *Question 9*).

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

The FTC's Behavioural Advertising Principles suggest website operators should obtain affirmative express consent before using sensitive consumer data (*see Question 9*).

The GLB Act does not specifically address individual categories of data, however, regulators have also implemented response programme regulations requiring the financial institutions to notify the regulator (and in some cases the customer) when there has been unauthorised access to sensitive customer information.

A law relating to GLB, the Fair Credit Reporting Act (15 U.S.C. §1681), limits how consumer reports and credit card account numbers can be used and disclosed. Financial institutions are prohibited from disclosing an account number to a non-affiliated entity (other than a consumer reporting agency) for telemarketing, e-mail marketing or direct marketing purposes.

Under the HIPAA, there are specific rules regulating the disclosure of psychotherapy notes. A covered entity must generally obtain written authorisation before disclosing psychotherapy notes, even for purposes of medical treatment, medical operations or payment.

There are several California laws that provide special rules in relation to the processing, collection, transmission and disclosure of certain types of data including, without limitation:

- Financial and medical data.
- Social security numbers.
- Credit card account numbers.
- Telecommunications records.
- Radio frequency identification (RFID).
- Library records.

Rights of individuals

12. What information should be provided to data subjects at the point of collection of the personal data?

For the FTC's Behavioural Advertising Principles' recommended practices, see *Question 7*.

The GLB Act requires a financial institution to provide notice of its privacy practices, but the timing and content of this notice depends on whether the data subject is a consumer or a customer. A customer (someone with an established and ongoing relationship with the financial institution) is entitled to receive the financial institution's

privacy notice when the relationship is established and annually after that. The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices. It should describe:

- The categories of information that it collects and discloses.
- The categories of affiliated and non-affiliated entities with whom it shares information.
- That the consumer or customer has the right to opt out of some disclosures (see *Question 6* for details about when an opt-out is required).
- How the consumer or customer can exercise the opt-out right (if an opt-out right is available).

HIPAA requires covered entities to provide a notice of privacy practices to data subjects, generally on the first visit for treatment. The notice must contain the statement: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY". The notice must describe:

- The uses and disclosures of PHI the covered entity is entitled to make (such as to receive payment from an insurance company).
- How an individual can access his information.
- How to complain about an HIPAA violation.
- An effective date.

Covered entities are not required to register with a governmental agency, but covered entities must keep records of certain disclosures of PHI.

The California Security Breach Notification Law does not specifically address information that should be provided to data subjects at the point of collection, as it focuses on requirements of disclosure of security breaches.

The privacy policy required under the California Online Privacy Protection Act must:

- Identify the categories of personally identifiable information that the operator collects through the website or online service and the categories of third-party persons or entities with whom the operator can share that personally identifiable information.
- Explain how a consumer can review his personal information collected by the operator of the website or online service, and how the consumer can make changes to that information, if the website or online service operator allows this.
- Explain how the website or online service operator notifies consumers of changes to its privacy policy.
- State the effective date of the privacy policy.

13. What other specific rights are granted to data subjects?

The FTC Act and most US privacy laws (except the HIPAA and some California laws) do not generally provide data subjects with specific access rights to their data. However, the Children's Online Privacy Protection Act allows a parent to view the personal information collected by a website about a child, and to delete and correct that information.

The GLB Act allows consumers or customers to opt-out of certain disclosures but does not generally specifically provide access rights to these individuals. In some cases, financial institutions must notify the customer when there has been unauthorised access to his sensitive customer information.

Under the HIPAA, a data subject has the right to request access to and to make corrections to his own PHI, and can (with some exceptions) request an account of the manner in which his PHI has been used or disclosed.

The California Shine the Light Law, Civil Code §§1798.83 to 1798.84 allows consumers to learn how their personal information is shared by companies for marketing purposes and encourages businesses to let their customers opt out of this. In response to a customer request, a business must provide either:

- A list of the categories of personal information disclosed to other companies for their marketing purposes during the preceding calendar year, with the companies' names and addresses.
- A privacy statement giving the customer a cost-free opportunity to opt out of this information sharing.

Financial services companies subject to the California Financial Information Privacy Act are exempted from this law.

California's student privacy law, Cal. Bus. and Prof. Code §22584, prohibits an operator of an Internet website, online service, online application, or mobile application from knowingly engaging in targeted advertising to students or their parents or legal guardians, using covered information to amass a profile about a K–12 student, selling a student’s information, or disclosing covered information.

14. Do data subjects have a right to request the deletion of their data?

Data subjects currently have no right to request the deletion of their data under applicable federal laws. Under the HIPAA, an individual can request that inaccurate or incomplete information is amended, however, the covered entity need not amend the data.

The California Online Privacy Protection Act requires operators of web sites, online services and mobile apps that are directed to minors, or that have actual knowledge that a minor is using their site or service, to permit a minor who is a registered user to remove or request the removal of certain online information that the user posted. The law does not require companies to remove data from their servers, as long as they delete it from their websites, and the law does not apply to content for which the minor 'received compensation or other consideration.'

Security requirements

15. What security requirements are imposed in relation to personal data?

The FTC's Behavioural Advertising Principles suggest that website operators that collect and/or store consumer data for behavioural advertising should provide reasonable security for that data and should retain data only as long as is necessary to fulfil a legitimate business or law enforcement need. Consumer data protection should be based on the:

- Sensitivity of the data.
- Nature of the company's business operations.
- Types of risk a company faces.
- Reasonable protections available to a company.

The GLB Safeguards Rule requires companies to develop a written information security plan that describes their customer information protection programme. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- Designate one or more employees to co-ordinate its information security programme.
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks.
- Design and implement a safeguards programme, and regularly monitor and test it.
- Select service providers that can maintain appropriate safeguards, ensure contracts require them to maintain safeguards, and oversee their handling of customer information.
- Evaluate and adjust the programme in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are designed to be flexible. According to the FTC, companies should implement safeguards appropriate to their own circumstances. The FTC's Disposal Rule regulates the destruction of consumer reports. The recently issued Red Flags Rules require financial institutions and creditors to develop a written programme that identifies and detects the relevant warning signs (red flags) of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The programme must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the programme.

The HIPAA requires covered entities to:

- Use and disclose the minimum amount of PHI necessary to complete a transaction.

- Implement data security procedures and policies to protect data.
- Comply with certain standards established for electronic transactions.

There is also Guidance for Remote Use of and Access to Electronic Protected Health Information that specifically addresses the risks associated with storing, accessing and transferring medical data on laptop computers, wireless devices, home computers, flash drives, e-mail and public workstations.

The California Security Breach Notification Law is triggered by unauthorised disclosure of unencrypted information, so it encourages companies to encrypt the personal information of Californians. The law was amended in 2015, by A.B. 864, which defines information as encrypted if it is rendered unusable, unreadable, or indecipherable to an unauthorised person through a security technology or methodology generally accepted in the field of information security. The amendment, which went into effect on 1 January 2016, does not specify a particular encryption methodology but defines acceptable practices in terms of industry norms.

For California Online Privacy Protection Act requirements, see *Question 4*. For the requirements for these privacy policies, see *Question 12*.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

48 states and the District of Columbia, Puerto Rico and the US Virgin Islands have enacted security breach notification laws. There is no federal security breach notification law, although federal bills calling for such legislation have been proposed each year for several years. State security breach notification laws typically require any person or business that owns or licenses computerised data including personal information to disclose any breach of the system security to all residents whose unencrypted personal information was acquired by an unauthorised person. These laws may also require notification to state Attorneys General. Notification can be by e-mail, post, or in state-wide media, depending on the number of affected individuals. Most laws allow an entity to delay notification for law enforcement purposes.

The HIPAA also requires certain entities including health plans and health care providers to notify individuals when their unsecured personal health information has been breached (*see 45 CFR Parts 160 and 164*).

National banking regulators issued guidance encouraging certain financial institutions to notify customers if an institution determines that misuse of customer information has occurred, and to notify the appropriate banking regulator as soon as possible (Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 CFR Part 30, 12 CFR Parts 208 and 225, 12 CFR Part 364, and 12 CFR Parts 568 and 570, issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision).

Processing by third parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The FTC has issued several rules, including the Safeguards Rule, the Affiliate Sharing Rule, and the Affiliate Marketing Rule, that limit the sharing and use of financial information and credit report information with affiliates.

Under GLB, a financial institution can disclose an individual's non-public personal information with a non-affiliated entity without providing the individual the right to opt out if:

- The disclosure is to a third party that uses the information to perform services for the financial institution.
- The financial institution provides notice of this practice to the individual before sharing the information.
- The financial institution and the third party enter into a contract that requires the third party to maintain the confidentiality of the information and to use the information only for the prescribed purpose.

The HIPAA Privacy Rule allows covered entities to disclose PHI to business associates if the parties enter into an agreement that requires the business associate to agree to use the information only for the purposes for which it was engaged by the covered entity, to safeguard the information from misuse, and to assist the covered entity comply with certain of the covered entity's duties under the Privacy Rule. When a covered entity knows of a material breach or violation by the business associate of the agreement, the covered entity must take reasonable steps to cure the breach or end the violation, and if these steps are unsuccessful, to terminate the arrangement. If termination of the agreement is not feasible, a covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights.

Under the California Security Breach Notification Law, a third party that maintains computerised data including personal information the third party does not own must notify the owner or licensee of the information of any breach of data security immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorised person. California law also provides that a business that discloses personal information about a Californian under a contract with a non-affiliated third party must contractually require the third party to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorised access, destruction, use, modification or disclosure.

For California Online Privacy Protection Act requirements, see *Question 4*. The information handling procedures includes disclosure of third parties, to whom personal information is transferred.

Electronic communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The FTC's Behavioural Advertising Principles are voluntary in nature. These principles suggest that website operators:

- Disclose their data collection practices tied to online behavioural advertising which rely on the use of cookies.
- Obtain affirmative consent before collecting sensitive information.
- Disclose that consumers can opt out of these practices.
- Provide a mechanism for opting out.

The advertising industry has also created a self-regulatory programme that mirrors the FTC's suggestions. The Digital Advertising Alliance (DAA) issued self-regulatory principles and in 2013 announced compliance decisions. Several decisions involved companies that failed to provide both kinds of notice, on the webpage where data is collected and on the webpage where an advertisement is displayed based on the data that was collected. Other compliance actions have resulted from websites that offered an opt-out but did not honour that opt-out for a minimum of five years.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

The CAN-SPAM Act is the federal anti-spam law that applies very broadly to commercial e-mail in the US (codified at 15 U.S.C. §§7701-7713 and at 18 U.S.C. §1037). FTC Rules implementing CAN-SPAM are collected at 16 CFR Part 316. Federal Communications Commission Rules regarding text messages that are subject to CAN-SPAM are in 47 CFR 64.3100.

CAN-SPAM addresses two types of e-mail:

- **Commercial e-mail.** This is defined as any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an internet website operated for a commercial purpose).
- **A transactional or relationship message.** This is a message whose primary purpose is to:
  - facilitate, complete or confirm a commercial transaction that the recipient previously agreed to enter into with the sender;
  - provide product warranty, product recall or safety information concerning a product purchased by the recipient;
  - provide account information or employment or related benefit plan information;
  - to deliver goods or services, or updates or upgrades that the recipient is entitled to receive pursuant to a transaction previously entered into with the sender.

Commercial e-mail must include the following:

- Accurate and non-misleading routing and header information, that is, "From", "To", and "Reply To" fields.
- A "Subject" line that is not deceptive.
- A notice that the recipient has the right to opt out of receiving future e-mail messages from the sender. The law does not specify where the notice must appear, but it must be clear and conspicuous. The recipient should not have to search the message to find it.
- An internet-based opt-out mechanism capable of receiving opt-out requests for at least 30 days after transmission of the message. The sender must honour an opt-out request within ten business days.
- A clear and conspicuous identification that the e-mail is an advertisement or solicitation. This requirement does not apply if the sender has the recipient's affirmative consent to send commercial e-mail. Affirmative consent requires that the recipient expressly consented to receive commercial e-mail from the sender. If the sender does not have the recipient's affirmative consent, the e-mail must be identified as an advertisement or solicitation. A sender does not have to actually use the words advertisement or solicitation, but the message must clearly be identified as a commercial offer. Phrases such as "you may be interested in this great offer" or "for a limited time, we are offering special rates" would probably suffice, if conspicuously included.
- The sender's physical postal address (PO boxes and commercial mail drops that meet certain US Postal Service requirements suffice as a sender's physical postal address).

All transactional or relationship messages must include accurate and non-misleading routing information. For example, the "From" and "To" lines must not be misleading.

CAN-SPAM imposes obligations on senders and initiators. A sender is the person or entity who initiates a commercial e-mail message and whose product, service or website is advertised or promoted by the message. Some e-mails, such as in a co-branded promotion, can have multiple senders, all of whom must comply with CAN-SPAM requirements. An initiator is the person or entity who originates or transmits a commercial e-mail message, but does not include the service that is responsible solely for the routine conveyance of the message. Multiple persons or entities can qualify as initiators and can therefore all be subject to CAN-SPAM requirements.

Each separate e-mail in violation of the law is subject to penalties of up to US$16,000, and more than one person can be held responsible for violations. For example, both the company whose product is promoted in the message and the company that originated the message can be legally responsible. E-mail that makes misleading claims about products or services can also be subject to laws outlawing deceptive advertising, such as section 5 of the FTC Act.

The CAN-SPAM Act has certain aggravated violations that can give rise to additional fines. The law provides for criminal penalties, including imprisonment, for:

- Accessing someone else's computer to send spam without permission.
- Using false information to register for multiple e-mail accounts or domain names.
- Relaying or retransmitting multiple spam messages through a computer to mislead others about the origin of the message.
- Harvesting e-mail addresses or generating them through a dictionary attack (sending e-mail to addresses made up of random letters and numbers in the hope of reaching valid ones).
- Taking advantage of open relays or open proxies without permission.

International transfer of data

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

There are few limits on the transfer of personal data outside the US. Several states have enacted laws that limit or discourage state agencies or state contractors from outsourcing data processing beyond US borders, but these laws are typically limited to state government agencies and private companies that contract to perform services for or provide goods to state agencies.

However, the position of the FTC and other regulators is that the applicable US laws and regulations still apply to the data after it leaves the US, and US regulated entities remain liable for:

- Data exported out of the US.
- The processing of data overseas by subcontractors.
- Subcontractors using the same protections (such as through the use of security safeguards, protocols, audits and contractual provisions) for the regulated data when it leaves the country.

21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?

There are few express restrictions on storing personal data outside the US, but some states have restrictions on data access, maintenance and processing from outside the US with respect to government contracts and off-shore outsourcing situations. (Some federal agencies can also impose such restrictions in their contracts.) Otherwise, a requirement to store personal data in the US usually manifests as a contractual requirement where a customer is apprehensive about sensitive data being stored in jurisdictions which are perceived as having a weak personal data protection regime.

Data transfer agreements

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

For years, many US companies engaging in cross-border transfers of personal data between Europe and the US had relied on the EU-US Safe Harbour programme, using European Commission (Commission) approved model contracts, or for multinationals, implementing binding corporate rules (BCRs). The Safe Harbour programme was developed by the US Department of Commerce and the Commission to address the Commission's determination that the US does not have in place a regulatory framework that provides adequate protection for personal data transferred from the European Economic Area (EEA).

In October 2015, Europe's highest court struck down the established Safe Harbour framework in its Schrems v. Facebook ruling. In light of the ruling, companies could no longer rely on self-certification to establish compliance with EU privacy laws. European and American regulators scrambled to find an alternative framework for trans-Atlantic data transfers and in February 2016, the US Department of Commerce and the European Commission released a new "Privacy Shield" framework, which was intended to create more robust, enforceable rights protecting data transfers. Although the EU Article 29 Working Party expressed concerns, the European Commission adopted the EU-US Privacy Shield on 12 July 2016. The Privacy Shield imposes **s**trong obligations on companies handling data; clear safeguards and transparency obligations on US government access; effective protection of individual rights; and an annual joint review mechanism.

In addition, Congress passed the Judicial Redress Act in February 2016 to give additional civil remedies for citizens of EU member states. The Act allows citizens of ally countries (and organisations, such as the EU) to bring civil actions under the Privacy Act of 1974 for unlawful disclosure of their personal records by US government agencies.

Under GLB, before a financial institution transfers any non-public personal information, it must disclose its privacy notice and provide the individual with the opportunity to opt out of certain non-affiliated third party sharing (whether the transfer is within or outside of the US).

The HIPAA Transactions Rule covers trading partner agreements involving the exchange of information in electronic transactions. The Department of Health and Human Services has provided sample business associate agreements, but these are provided as guidance and covered entities are not required to use these sample agreements.

The California Security Breach Notification Law requires the disclosure of security breaches, but does not specifically address the use of data transfer agreements.

For California Online Privacy Protection Act requirements, see *Question 4*, but these do not specifically address the use of data transfer agreements.

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

For the FTC's Behavioural Advertising Principles' recommended practices, see *Question 7*.

The GLB Act requires a financial institution to disclose to a customer its privacy practices and provide the customer an opportunity to opt-out of certain disclosures before transferring any non-public personal information. Because the mechanism required is an opt-out provision as opposed to an opt-in, an individual must take affirmative action to stop the transfer.

Under the HIPAA, if a business associate has signed a business associate agreement that is HIPAA compliant, and the disclosure of PHI is otherwise permitted without obtaining consent from the data subject, the agreement is generally sufficient to effect the transfer. Trading partner agreements are generally used to address the technology-relation obligations of the parties to a transaction and are generally insufficient to legitimise a transfer, where authorisation is otherwise required.

The California Security Breach Notification Law requires disclosure of security breaches, but does not specifically address the use of data transfer agreements.

For California Online Privacy Protection Act requirements, see *Question 4*, but these do not specifically address the use of data transfer agreements.

24. Does the relevant national regulator need to approve the data transfer agreement?

The GLB Act does not require that a national regulator approve a data transfer agreement.

The HIPAA does not require that a national regulator approve a data transfer agreement, although a regulator may have audit powers to ensure compliance with HIPAA rules.

The California Security Breach Notification Law does not specifically address the use of data transfer agreements.

The California Online Privacy Protection Act does not specifically address the use of data transfer agreements.

Enforcement and sanctions

25. What are the enforcement powers of the national regulator?

The FTC is the primary US enforcer of national privacy laws. Although other national agencies (such as the banking agencies) are authorised to enforce various privacy laws, the FTC brings considerably more enforcement actions than the other agencies. The FTC can initiate an investigation, issue a cease and desist order, and file a complaint in court. The FTC also reports to Congress on privacy issues and recommends the enactment of required privacy legislation.

The GLB Act is enforced by the FTC, federal banking agencies, and state insurance agencies, although the FTC is more active as an enforcer than the other agencies.

The HIPAA is enforced by the Office of Civil Rights within the Department of Health and Human Services. This office can initiate an investigation into a covered entities information handling practises to determine whether it is complying with the HIPAA Privacy Rule, and allows individuals to file complaints about privacy violations.

The California Security Breach Notification Law and the California Online Privacy Protection Act are enforced by the California Attorney General and district attorneys.

26. What are the sanctions and remedies for non-compliance with data protection laws?

The FTC Act provides penalties of up to US$16,000 for each offence. The FTC can also obtain an injunction, restitution to consumers, and repayment of investigation and prosecution costs. Criminal penalties include imprisonment for up to ten years. In 2006, a data broker agreed to pay US$15 million to settle charges filed by the FTC for failing to adequately protect the data of millions of consumers. Settlements with government agencies can also include onerous reporting requirements, audits and monitoring by third-parties. A major retailer that settled charges of failing to adequately protect customer's credit card numbers agreed to allow comprehensive audits of its data security system for 20 years.

Penalties for violations of the GLB Act are determined by the authorising statute of the agency that brings the enforcement action. For example, an enforcement action brought by the FTC could include penalties of up to US $16,000 per offence. Individuals who obtain, attempt to obtain, cause to be disclosed or attempt to cause to be disclosed customer information of a financial institution relating to another person through a false, fictitious or fraudulent means, can be subject to fines and/or imprisoned for up to five years. In addition, there are criminal penalties for the perpetrator of up to ten years in prison and fines of up to US$500,000 (for an individual) and US $1 million (for a company) if such acts are committed or attempted while violating another US law or as part of a pattern of illegal activity involving more than US$100,000 in a year.

The HIPAA authorises civil penalties ranging from US$100 to US$1.5 million, depending on a number of factors, including whether the operator knew the act was a violation, whether the violation was quickly corrected and whether the operator was wilfully negligent. Criminal penalties can increase to US$250,000 and/or up to ten years in jail if the offence was committed under false pretences or with intent to sell the data for commercial gain.

Some state and federal laws allow individuals to sue in court for privacy violations, including classes of individuals, and these can also result in significant fines or damages awards. One of the largest data security breaches to date in the US occurred in late 2013 at Target stores. This data breach may have disclosed the payment card information of over 40 million consumers and the personal information of an additional 70 million consumers. Target was sued by consumers and by shareholders, and was investigated by Congress and state Attorneys General. The second largest data breach is reported to have cost a major retailer at least US$256 million and perhaps up to US$500 million. The company discovered that credit and debit card numbers of over 45 million consumers were stolen and used to make purchases and open fake accounts. The company settled several class action law suits filed by consumers as well as law suits filed by credit card companies and banks that had to reissue millions of cards. On 23 May 2017, Target agreed to pay US$18.5 million to settle investigations by 47 states and the District of Columbia into the 2013 customer data breach. This is the largest multistate data breach settlement in history.

The Ponemon Institute calculated that in 2016 the average cost of a security breach to a company was US$4 million up from US$3.79 million in 2015. Breach prevention and notification is an increasingly costly proposition, with a 12% increase in per capita cost just since 2013. In addition to civil and criminal sanctions, security breaches can

have far reaching consequences for companies in terms of loss of customer confidence and trust, customer churn, and loss of revenue, market share, brand and shareholder value.

Regulator details

Federal Trade Commission (FTC)
W *www.ftc.gov*

Main areas of responsibility. The FTC enforces the FTC Act, various rules and guidelines relating to commerce and privacy.

Department of Health and Human Services (HHS) Office of Civil Rights
W *www.hhs.gov/ocr/privacy/index.html*

Main areas of responsibility. The HHS Office of Civil Rights enforces HIPAA.

The California Attorney General
W *http://oag.ca.gov/*

Main areas of responsibility. The California Attorney General enforces all California laws including laws relating to commerce and privacy.

Online resources

The Federal Trade Commission Act
W *www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I*

Description. Unofficial website maintained by Cornell Law School with up-to-date text of Federal Trade Commission Act.

Title V of Gramm-Leach-Bliley (GLB) Act

W *www.law.cornell.edu/uscode/text/15/6801*

Description. Unofficial website maintained by Cornell Law School with up-to-date text of Title V of Gramm-Leach-Bliley (GLB) Act.

Health Information Privacy

W *www.hhs.gov/ocr/privacy/index.html*

Description. Official website containing the text of the Health Insurance Portability and Accountability Act (HIPAA) and various rules and guidelines, updated frequently.

FTC's Self-Regulatory Principles for Online Behavioral Advertising

W*www.ftc.gov/os/2009/02/P085400behavadreport.pdf*

Description. Official up-to-date version of FTC's Self-Regulatory Principles for Online Behavioral Advertising.

Children's Online Privacy Protection Act

W *www.ftc.gov/ogc/coppa1.htm*

Description. Official up-to-date version of Children's Online Privacy Protection Act.

Electronic Code of Federal Regulations

W *www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=fa34927e2ade43c1645fe450ea95d368&rgn=div5&view=text&node=16:1.0.1.3.36&idno=16*

Description. Official version of FTC COPPA Rule, updated whenever the Rule is amended.

State of California Department of Justice
W *http://oag.ca.gov/privacy/privacy-laws*

Description. Official website of California Office of Privacy Protection which provides up-to-date text of all California and selected Federal privacy laws.

Contributor details

Ieuan Jolly, Partner

Loeb & Loeb LLP

T +1 212 407 4810
F +1 646 390 0403
E *ijolly@loeb.com*
W *www.loeb.com*

Areas of practice. Privacy; cybersecurity; data optimisation and technology-enabled transactions.

Statement of the U.S. Chamber of Commerce

ON: Cybersecurity of the Internet of Things

TO: House Oversight and Government Reform Committee Information Technology Subcommittee

DATE: October 3, 2017

1615 H Street NW | Washington, DC | 20062

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations. The Chamber is dedicated to promoting, protecting, and defending America's free enterprise system.

More than 96% of Chamber member companies have fewer than 100 employees, and many of the nation's largest companies are active members. We are therefore cognizant not only of the challenges facing smaller businesses but also those facing the business community at large.

Besides representing a cross-section of the American business community with respect to the number of employees, major classifications of American business—for example, manufacturing, retailing, services, construction, wholesalers, and finance—are represented. The Chamber has membership in all 50 states.

The Chamber's international reach is substantial as well. We believe that global interdependence provides opportunities, not threats. In addition to the American Chambers of Commerce abroad, an increasing number of our members engage in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Matthew J. Eggers
Executive Director, Cybersecurity Policy, U.S. Chamber of Commerce
House Oversight and Government Reform Committee
Information Technology Subcommittee
Cybersecurity of the Internet of Things
October 3, 2017

Good afternoon, Chairman Hurd, Ranking Member Kelly, and other distinguished members of the Information Technology Subcommittee (subcommittee). My name is Matthew Eggers, and I am the executive director of cybersecurity policy with the U.S. Chamber's National Security and Emergency Preparedness Department. On behalf of the Chamber, I appreciate the opportunity to testify before the subcommittee regarding *Cybersecurity of the Internet of Things*. The Chamber welcomes the Subcommittee's dedication to examining leading cyber matters.

The Chamber's National Security and Emergency Preparedness Department was established in 2003 to develop and implement the Chamber's homeland and national security policies. The department's Cybersecurity Working Group (CWG), which I lead, identifies current and emerging issues, crafts policies and positions, and provides analysis and direct advocacy to government and business leaders.

In addition to the CWG, I want to highlight two other groups within the Chamber that handle Internet of Things (IoT) issues, including our Chamber Technology Engagement Center (C_TEC) and Global Information Security Working Group (GISWG). First, C_TEC is at the forefront of advancing IoT deployment and innovation in the digital economy.[1] Among its initiatives are working groups on unmanned aerial vehicles, IoT, and autonomous vehicles.[2]

Second, the GISWG pushes the Chamber's views to international audiences, including calling on countries and regions to align their cybersecurity governance programs with the joint industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (the framework). It also urges the protected sharing of cyber threat data among multiple public and private parties.

The GISWG and six European organizations recently sent a letter to the European Commission regarding "measures on cybersecurity standards, certification and labelling to make ICT-based systems, including connected objects." The industry groups argued that Europe, like the U.S., can expect to benefit from economic growth brought about by the expanding IoT as long as policymakers cultivate a digital environment that avoids misguided regulations and supports pioneering businesses.[3] Underpinning the Chamber's efforts at home and abroad is advocacy for smart policies for smart devices.

I recognize that the Subcommittee is considering legislation comparable to S.1691, the IoT Cybersecurity Improvement Act of 2017. The Chamber is reviewing the legislation with our members and welcomes having a constructive dialogue with the subcommittee and its staff. Still, I will confine my written statement to the Chamber's thinking on the IoT and cybersecurity.

Summary: The Internet of Things (IoT) Will Further Economic Growth; Smart Risk Management Principles and Policies Are Fundamental to Sound Security

The U.S. Chamber of Commerce is optimistic about the future of the IoT, which continues the decades-long trend of connecting networks of objects through the internet. The IoT will significantly affect many aspects of the economy, and the Chamber wants to constructively shape the breadth and nature of its eventual impact. Indeed, many observers predict that the expansion of the IoT will bring positive benefits through enhanced integration, efficiency, and productivity across many sectors of the U.S. and global economies.

Meaningful aspects of the IoT, including guarding against botnets and other automated threats, will also influence economic growth, infrastructure and cities, and individual consumers.[4] Fundamental cyber principles the Chamber will push to foster beneficial outcomes of the IoT are as follows:

- The IoT is incredibly complex, and there's no silver bullet to cybersecurity.
- Managing cyber risk across the internet and communications ecosystem is central to growing the IoT and increasing businesses' gains.
- The business community will promote policies favorable to the security and competitiveness of the digital ecosystem.
- IoT cybersecurity is best when it's embedded in global and industry-driven standards.
- Public-private collaboration needs to advance industry interests.

Overview: The Rapidly Emerging IoT Is Composed of Physical Things and Services

Descriptions of the IoT vary across stakeholders, yet the IoT generally refers to networks of objects that communicate with other objects and with computers through the internet.[5] The things may include virtually any object (e.g., a motion sensor) for which remote communication, data collection, or control may be useful—including vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, and agricultural systems. The emerging IoT may also more broadly affect economic growth, infrastructure and cities, and individual consumers.

To be sure, the IoT is more than just physical things. It includes services (e.g., smartphone applications) that support and depend on devices, as well as the connections among the devices, networks, and systems. In other words, the IoT potentially involves vast numbers and types of interconnections between objects and systems. It is widely considered the next major stage in the evolution of cyberspace.[6]

The Chamber views the IoT as composed of two major segments—consumer IoT and industrial IoT.[7] There is also a distinction emerging between managed and unmanaged IoT, in

which some IoT services and devices are consumer deployed, while others are part of value-added services and products administered by third-party providers (e.g., cloud-based platforms).

The Chamber believes the revolutionary benefits of the IoT will be realized only in an environment that prioritizes specific activities by industry and government, particularly managing cyber risk and avoiding regulations that would stunt IoT innovation and deployments.[8] The federal government, led by the Department of Commerce, should strive toward public-private collaboration, interagency coordination, and global engagement, especially with respect to standardization.[9]

The IoT is incredibly complex, and there's no one-size-fits-all solution to cybersecurity. The myriad, fast-moving threats that seek to compromise the IoT are borderless and include nation-states, organized crime, hacktivists, and terrorists that businesses cannot tackle alone.

Managing Risk Across the Internet and Communications Ecosystem Is Key to Growing the IoT and Increasing Businesses' Gains

Many companies go to great lengths to incorporate security into the design phase of IoT devices and services they sell globally. The Chamber wants device makers, service providers, and buyers to gain from the business community leading the development of state-of-the-art IoT components and leveraging sound risk management approaches in diverse settings such as manufacturing, transportation, energy, and health care.

Strong IoT security should be a win-win proposition for makers, providers, and purchasers.[10] Indeed, the IoT could dramatically unleash significant economic growth across the country and the world. According to a frequently cited report, approximately 50 billion devices will be connected to the internet by 2020. According to the Chamber's estimates, the IoT could add roughly $15 trillion to global GDP over the next 20 years. By other accounts, the IoT could have a cumulative economic impact of $3.9 trillion to $11 trillion per year by 2025.[11]

Sound private sector-led IoT risk management initiatives can create a virtuous cycle of security in which consumers seek out secure devices and services, and industry stakeholders prioritize security in the design, production, and improvement phases of their offerings. Different sets of flexible cybersecurity best practices will be relevant for different IoT audiences, ranging from producers to network operators to users.

The Chamber, which has members operating throughout the entire IoT landscape, urges IoT stakeholders to mitigate risks in this technological environment so that hazards to businesses' cybersecurity do not pool at any given point. Unmitigated risk and threats could create perils not only for companies and sectors but for the IoT at large.[12]

To be sure, the private sector is not standing still in the face of increased risk from the IoT. A Gartner report says, "Worldwide spending on [IoT] security will reach $348 million in 2016, a 23.7% increase from 2015 spending of $281.5 million. In addition, spending on IoT security is expected to reach $547 million in 2018.[13] By 2020, Gartner predicts that over half of all IoT implementations will use some form of cloud-based security service.

Solutions are being developed and offered globally. As a leading cybersecurity company explains, security architectures are being refined to support comprehensive security because "IoT systems are often highly complex, requiring end-to-end security solutions that span cloud and connectivity layers, and support resource-constrained IoT devices that often aren't powerful enough to support traditional security solutions."[14] Increased attention is being paid to authentication and encryption. All of these measurers will improve security in the IoT, and it is vital that these innovations have a global reach.

Industry Will Promote Policies Favorable to the Security and Competitiveness of the Digital Ecosystem

Regulatory relief and reform are at the top of the Chamber's 2017 growth agenda. Businesses cannot expand and create jobs if they are burdened by complex and expensive regulations.[15] The vast potential of the IoT will be realized only in a hospitable policy climate. The explosive growth of the internet in the 1990s resulted from a minimal regulatory environment, which has been the foundation for U.S. global internet leadership.

Today, leading industry stakeholders are more attuned to the importance that cybersecurity brings to the marketplace.[16] While perfect security of network-connected devices is ambitious, the Chamber urges all stakeholders to make the cybersecurity of the IoT a priority—not simply for security's own sake but for the end-to-end well-being of the IoT ecosystem.[17]

The Chamber believes IoT-specific mandates or guidance, including ones related to security and privacy, are unnecessary.[18] As with other areas of cybersecurity (e.g., critical infrastructure), prescriptive legislation and regulations will have negative consequences on businesses and consumers. For example, IoT-related security mandates will slow innovation and quickly become obsolete compared with threat actors that can circumvent compliance-based regimes. The Chamber will push back against governmental actions that attempt to restrict a rapidly evolving field like the IoT.[19]

Further, overlapping and/or conflicting red tape at the federal, state, and local levels will impose unnecessary costs on businesses and erode the economies of scale needed for successful IoT penetration across the economy. So, too, fragmented national cybersecurity regimes will threaten important policy goals such as fostering the international interoperability of the internet and connected technologies and establishing meaningful information-sharing relationships among multiple public and private parties.

Maureen Ohlhausen, commissioner of the Federal Trade Commission, put it well when she said, "It is thus vital that government officials, like myself, approach new technologies with a dose of *regulatory humility* [italics added]."[20] In a similar vein, it's constructive that the FTC has said in its writings, "[T]here is great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature."[21]

Any policy effort needs to urge greater awareness by consumers about cybersecurity. Users will be a critical part of securing the IoT, given the swift pace of technical innovation and

the speed of IoT availability in the marketplace.[22] Buyers need to manage their devices, use passwords and other security-enhancing tools, accept provider updates, and be knowledgeable about connectivity security (e.g., Wi-Fi), among other cybersecurity basics.

IoT innovators are concerned about liability, which is a real threat and could negatively affect innovation.[23] Fears expressed by some about IoT security have been exploited by opportunists to target companies that make sound investments in the IoT. Such claims can lead to nonmeritorious lawsuits. For instance, certain vulnerability disclosures have led to class action suits, even when no unauthorized intrusion of a technology product or system occurred. And with the benefit of hindsight, alleged security issues can be the basis for unwarranted claims against industry regarding deception or unreasonable practices.[24]

Instead of pursuing punitive measures, policymakers should look for creative ways to reduce barriers to innovation and limit undue risk of liability to encourage desired information sharing, communication, and product development.

IoT Cybersecurity Is Best When Embedded in Global and Industry-Driven Standards

Cybersecurity standards and best practices are optimally led by the private sector and adopted on a voluntary basis. They are most effective when developed and recognized globally. Such an approach avoids burdening multinational enterprises and IoT adopters with the requirements of multiple, and often conflicting, jurisdictions.

Misplaced or unintended policy constraints will limit U.S. competitiveness in the global marketplace.[25] The Chamber welcomes the Department of Commerce's commitment to "advocate against attempts by governments to impose top-down, technology-specific 'solutions' to IoT standardization needs."[26]

International policymakers should align IoT security programs with industry-backed approaches to risk management, such as the framework. The framework is biased toward a standards- and technology-neutral approach to managing cyber risks. Moreover, policymakers need to support NIST's strategic engagement in international standardization to attain U.S. cyber objectives.[27]

Public-Private Collaboration Needs to Advance Industry Interests

Public-private partnerships are critical to addressing IoT cybersecurity.[28] Four examples highlight the importance of quality collaboration.[29] First, the NTIA's January 2017 *Green Paper: Fostering the Advancement of the Internet of Things* (the *Green Paper*) assesses what actions stakeholders should take to advance the IoT, including matters relating to cybersecurity.

The Chamber generally agrees with the agency's overall approach to public-private collaboration. "Over the past few decades in the United States," the NTIA observes, "[T]he role of government largely has been to establish and support an environment that allows technology to grow and thrive." Rather than intervening prematurely in the nascent, rapidly changing IoT marketplace, the NTIA's *Green Paper* stresses that the role of government is to establish and

support an environment that promotes the development and progress of emerging technologies by "[e]ncouraging private sector leadership in technology and standards development, and using a multistakeholder approach to policy making."[30]

Second, the NTIA is assembling a cybersecurity-focused multistakeholder process to address IoT security upgradability and patching of consumer devices that could prove helpful to interested parties. The Chamber believes the NTIA IoT security upgradability and patching effort and related activities can advance the private sector's interest in collaborative, voluntary best practices and shared information.

Third, NIST did an admirable job of convening many organizations to develop the framework. The Chamber believes the department is well positioned to convene stakeholders to identify existing standards and guidance to enhance the security and resilience of the IoT.[31]

Fourth, the Chamber recognizes the nonbinding principles the Department of Homeland Security put forward in its 2016 blueprint for securing the IoT across a range of design, manufacturing, and deployment activities. The Chamber looks forward to working with DHS leadership on improving the resilience of the IoT.[32]

***

The Chamber urges all stakeholders to play their parts to reduce risks associated with the growing IoT. Consumers need to demand secure devices and services. Companies that prioritize strong security should be rewarded through increased sales and market share. In addition, it is crucial that policymakers approach new IoT technologies with a dose of regulatory humility. There is abundant potential for innovation in this space. Legislation and other policies targeted specifically at the IoT could be detrimental to the creation of leading-edge products and services.

Endnotes

---

[1] The Chamber Technology Engagement Center (C_TEC) strongly supports H.R. 686, the DIGIT Act. Adoption of this bipartisan legislation would be a critical first step in the public-private development of a national IoT strategy based on data and real-world experiences. The DIGIT Act would also bring together stakeholders in government and industry to shape policy, helping ensure that the U.S. realizes the full economic potential of IoT and remains a leader in this next chapter of the internet.
www.congress.gov/bill/115th-congress/house-bill/686/cosponsors

[2] www.uschamber.com/ctec

[3] See August 16, 2017, letter to European Commission from the American Chamber of Commerce to the European Union (AmCham EU), the Confederation of Danish Enterprise, the Confederation of Danish Industry, the Confederation of Industry of the Czech Republic, EurElectric, the International Chamber of Commerce in Belgium, and the U.S. Chamber of Commerce.
www.uschamber.com/sites/default/files/iot.cybersecurity.coalition._ec.letter.pdf

[4] On July 28, 2017, the Chamber submitted comments to the National Telecommunications and Information Administration's (NTIA's) notice on *Promoting Stakeholder Action Against Botnets and Other Automated Threats*.

www.ntia.doc.gov/files/ntia/publications/us_chamber_letter_botnets_iot_cybersecurity_final.pdf

[5] The National Telecommunications and Information Administration's (NTIA's) January 2017 *Green Paper: Fostering the Advancement of the Internet of Things* is a significant policy paper regarding the development of the IoT. Some parties argue that strict definitions or labels could inadvertently narrow the scope of the IoT's potential applications (pg. 5). www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[6] Congressional Research Service (CRS), *The Internet of Things: Frequently Asked Questions* (October 13, 2015), R44227. https://fas.org/sgp/crs/misc/R44227.pdf

[7] See, in particular, comments filed with the NTIA by the C_TEC in March 2017 and June 2016.
www.ntia.doc.gov/files/ntia/publications/comments_of_c_tec_3-13-17.pdf
www.ntia.doc.gov/files/ntia/publications/cati.iotcommentsfinal.pdf

In March 2017, the Information Technology Industry Council (ITI) wrote to the NTIA concerning the *Green Paper* and said the IoT encompasses consumer IoT and industrial IoT. Consumer IoT devices include household appliances, wearables, and smartphones; industrial IoT devices include factory equipment, building systems, and digital signage (pg. 2). www.ntia.doc.gov/files/ntia/publications/iti.pdf

[8] See, especially, *The IoT Revolution and Our Digital Security: Principles for IoT Security*, September 19, 2017, written by the Chamber and Wiley Rein LLP. www.uschamber.com/IoT-security

[9] NTIA *Green Paper*, pgs. 11, 13.

[10] *2017 Cybersecurity Policy Priorities (Select Examples)*, Chamber's National Security and Emergency Preparedness Department (March 2017).
www.uschamber.com/sites/default/files/u.s._chamber_cyber_priorities_2017_short_version_final_march_2017.pdf

[11] www.ntia.doc.gov/files/ntia/publications/cati.iotcommentsfinal.pdf (pgs. 4–5)

[12] The Chamber's October 2016 *Statement on Encryption Policy and Cybersecurity* endorses robust encryption for information, including data at rest and data in motion.
www.uschamber.com/sites/default/files/documents/files/us_chamber_encryption-cyber_policy_statement_oct_14_2016_final_1_0.pdf

[13] *The IoT Revolution*, pg. 16; "Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016" (April 25, 2016). www.gartner.com/newsroom/id/3291817

[14] *The IoT Revolution*, pg. 16; Symantec, *An Internet of Things Reference Architecture* (2016).
www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

[15] Chamber's *2017 State of American Business Address* (January 11, 2017).
www.uschamber.com/speech/2017-state-american-business-address

Chamber's *The State of American Business: Fixing Our Broken Regulatory Process* (February 13, 2017)
www.uschamber.com/above-the-fold/the-state-american-business-fixing-our-broken-regulatory-process

[16] See, for example, IBM *Security's Five Indisputable Facts About IoT Security* (February 2017).
www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEF03018USEN.

The Broadband Internet Technical Advisory Group *Internet of Things (IoT) Security and Privacy Recommendations* (November 2016). www.bitag.org/report-internet-of-things-security-privacy-recommendations.php

[17] The National Security Telecommunications Advisory Committee (NSTAC) found that "IoT adoption will increase in both speed and scope, and that it will impact virtually all sectors of our society. The Nation's challenge is

ensuring that the IoT's adoption does not create undue risk. Additionally, the NSTAC determined that there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk." The *NSTAC Report to the President on the Internet of Things* (November 19, 2014), pg. ES-1. www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

Also see the opening statement of Rep. Fred Upton at a House Energy and Commerce joint Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology hearing, "Understanding the Role of Connected Devices in Recent Cyber Attacks" (November 16, 2016). http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-MState-U000031-20161116.pdf

Cisco noted in its March 2017 letter to the NTIA on the *Green Paper*, "As we gain greater experience managing the risks and benefits of [IoT] technologies, governments should continue to *forbear from developing regulatory approaches* to the IoT marketplace [italics added]" (pg. 7). www.ntia.doc.gov/files/ntia/publications/cisco_ntia_supplemental_iot_comments_03_13_2017_final.pdf

[18] Comments of the staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning in response to the NTIA's April 2016 notice and request for comments, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2016), pgs. 13–14. www.ntia.doc.gov/files/ntia/publications/p165403_ftc_staff_comment_before_ntia_in_docket_no_160331306-6306-01.pdf
www.ntia.doc.gov/files/ntia/publications/comments_of_c_tec_3-13-17.pdf

The IoT and cybersecurity do not raise novel privacy issues. The Chamber's comments on privacy are cited on pg. 31 of the NTIA *Green Paper*. We agree with ITI's March 2017 comments to the agency. ITI wrote that "a significant amount of IoT data will often have no connection to a person or individual. . . . [M]any of the privacy issues arising in the IoT context are nonetheless not new, as IoT applications where data on individuals is collected, the collection, use, sharing, and protection of such data are already subject to existing laws" (pgs. 4–5). www.ntia.doc.gov/files/ntia/publications/iti.pdf

[19] The NTIA *Green Paper* says, "Threats and vulnerabilities are constantly evolving. Predefined solutions quickly become obsolete or even provide bad actors with a roadmap for attack, the U.S. Chamber of Commerce noted. Many commenters stated that regulators must allow developers the flexibility to create cutting-edge improvements to defend their products and services and protect their users" (pg. 25).

In March 2017, USTelecom wrote to the NTIA on the *Green Paper* to say that the Department of Commerce and the NTIA "should encourage regulators to work with industry to identify potential cybersecurity gaps and distribute responsibilities across the broad ecosystem of device manufactures, applications developers, network service providers and others. Regulators . . . can *adopt more innovative and flexible means of collaboration* with industry [italics added]" (pg. 5). www.ntia.doc.gov/files/ntia/publications/ustelecom-comments-ntia-iot-2017-03-13-final.pdf

[20] Remarks of FTC Commissioner Maureen Ohlhausen, *Promoting an Internet of Inclusion: More Things AND More People, Consumer Electronics Show* (January 8, 2014), pgs. 1–2. www.ftc.gov/sites/default/files/documents/public_statements/promoting-internet-inclusion-more-things-more-people/140107ces-iot.pdf
www.ntia.doc.gov/files/ntia/publications/cati.iotcommentsfinal.pdf

[21] FTC staff report, *Internet of Things: Privacy & Security in a Connected World* (January 2015), pgs. vii, 49. www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[22] In its March 2017 comments to the NTIA regarding the *Green Paper*, Microsoft urged the Department of Commerce to acknowledge that basic cyber hygiene is a cybersecurity priority in the IoT space. "[M]any responsible technology providers ship patches on a regular basis, but users often fail to apply them," the company noted (pg. 5).

www.ntia.doc.gov/files/ntia/publications/microsoft_corporations_response_to_the_green_paper_-_march_2017.pdf

In its March 2017 letter to the NTIA pertaining to the *Green Paper*, Cisco noted the usefulness of the FTC's *Start with Security: A Guide for Business*, which distills practical lessons businesses can learn from the agency's casework on security.
www.ntia.doc.gov/files/ntia/publications/cisco_ntia_supplemental_iot_comments_03_13_2017_final.pdf

[23] In December 2016, the Commission on Enhancing National Cybersecurity's *Report on Securing and Growing the Digital Economy* called for the Department of Justice to lead an interagency study with the Department of Commerce and the Department of Homeland Security, among other agencies, and the private sector to "assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days" (pg. 25).
www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[24] In its March 2017 comments to NTIA on the *Green Paper*, the Security Industry Association said, "[T]here is a significant challenge not explicitly cited in the green paper—an uncertain or hostile legal environment that could deter IoT developers and limit the benefits of IoT devices for consumers. . . . IoT regulation by litigation is not a transparent or economically desirable policy solution to address concerns, and could be a serious impediment to growth and raise high-cost barriers to entry for small businesses" (pg. 3).
www.ntia.doc.gov/files/ntia/publications/iot_rpc_pt.2_sia.pdf

[25] "The knee-jerk reaction might be to regulate the Internet of Things, [but] . . . the question is whether we need a more holistic solution. *The United States can't regulate the world.* Standards applied to American-designed, American-manufactured, or American-sold device won't capture the millions of devices purchased by the billions of people around the world [italics added]."

This quote is taken from Rep. Greg Walden's opening remarks at a House Energy and Commerce joint Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology hearing, "Understanding the Role of Connected Devices in Recent Cyber Attacks"
(November 16, 2016).
http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-MState-W000791-20161116.pdf

[26] NTIA *Green Paper*, pg. 13.

[27] Chamber letter to NIST, *Draft Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (September 24, 2015).
www.uschamber.com/sites/default/files/september_24_2017_chamber_comments_draft_nistir_8074_intl_cyber_standardization_final.pdf

[28] In its March 2017 letter to the NTIA concerning the *Green Paper*, USTelecom wrote that it "supports the [Department of Commerce's] principle to convene stakeholders to address public policy challenges. In recent years, U.S. Government policy in an area of critical impact on IoT, namely cybersecurity, has been predicated on the assumption that a partnership between industry and government is superior to any prescriptive compliance regime, which, by its nature, would lack flexibility to respond promptly to new threats and potentially undermine security by providing the playbook for bad actors to exploit" (pg. 9).
www.ntia.doc.gov/files/ntia/publications/ustelecom-comments-ntia-iot-2017-03-13-final.pdf

[29] In its March 2017 comments to NTIA on the *Green Paper*, Samsung wrote, "[P]rivate sector leadership is critical to the success of the IoT in particular and technology growth and development in general. Yet collaboration between the government and private sector is essential to addressing challenges such as security and maintaining an open, global market for IoT technologies" (pg. 1).
www.ntia.doc.gov/files/ntia/publications/samsung_commerce-iot_comments_2017-03-13-c1.pdf

[30] NTIA *Green Paper*, pg. 2.

[31] In its March 2017 comments to the NTIA regarding the *Green Paper*, the American Cable Association said, "The NIST Cybersecurity Framework also provides a good model for the role of government in developing cybersecurity policies, as the Framework itself is the result of a highly collaborative effort between government and the private sector. While the government has a crucial role to play, it can be most helpful as a facilitator and convener—bringing together a diverse network of stakeholders to develop solutions" (pg. 5). https://www.ntia.doc.gov/files/ntia/publications/aca.pdf

[32] The Department of Homeland Security's paper says these principles are intended for IoT developers, IoT manufactures, service providers, and industrial and business-level consumers. See *Strategic Principles for Securing the Internet of Things (IoT), Version 1.0* (November 15, 2016). www.dhs.gov/securingtheIoT

ELECTRONIC DATA: A COMMENTARY ON THE LAW IN VIRGINIA IN 2007

The Honorable Thomas D. Horne *

I. INTRODUCTION

Just like the day we learned to ride a bike, most of us probably recall the day we were first introduced to the brave new world of computers. Little then did we realize, nor do we yet fully recognize, the power locked within the chip that processes our insatiable need for information. It is our good fortune that legal and ethical standards, rather than technology, continue to guide a principled approach to the practice of law. Computers and computer-generated data are tools only for processing information, a means to achieving an end result. Skilled advocacy and accurate decision-making depend on the collection and collation of information in a variety of forms. Now, electronic data provides the principal medium used in the pursuit of these goals.

Electronic data provides a lawyer with another source from which to obtain, retain, and disseminate information, albeit a different and novel source. Thus, it should be accorded a like dignity to that of handwritten and transcribed histories. However, the accuracy, cost, ease of recovery, and manageability of such data makes it an increasingly favored tool and target for the practitioner. So enchanted have some become with such data that clearly identifiable legal issues become clouded by bits and bytes of electronically maintained information. Litigation has become a

* Judge, 20th Judicial Circuit. B.A., Muhlenberg College; J.D., Marshall-Wythe School of Law, College of William and Mary. Judge Horne wishes to thank Erin M. Martinko (B.A., 1999, Cornell University; J.D., Candidate, 2008, George Mason University School of Law), Edward J. O'Shea, III (B.A., 1999, University of Pennsylvania; J.D., Candidate, 2008, George Mason University School of Law), and Joanne V. Frye (B.A., 2001, Washington & Jefferson College; J.D., 2004, University of Richmond School of Law).

search of the information universe about one's adversary, like a similarly ill-fated search for the fountain of youth.

This article addresses several issues related to the role of electronic data: how courts and legislatures wrestle with questions concerning digital information in an attempt to maintain stare decisis, current legislative attempts to respond to public policy concerns about such data, and the current expansion of the common law. Both the civil and criminal law are explored here, as well as vexing questions about jurisdiction, evidence, and cost. In each section, seminal cases and legislation are introduced and then expanded upon with a discussion of the relevant principles. Each review of a specific legal topic contains thoughts on the future course of this burgeoning area of the law.

Hopefully, the reader will take from this article a better understanding of how legal issues relating to electronic data may be approached and understood. Surprisingly, once the practitioner cuts through the shroud of science and follows Alice through the looking glass, existing legal concepts remain effective and are a constant reminder that law finds its strength in the harmonizing of the old with the new, stability and custom with social change.

Concerns for confidentiality, security, and a desire to communicate ideas to either a single person or to a vast audience portend a potent mixture for litigation. Applying extant rules and statutes to legal issues arising from new technologies is not easy. Traditional molds may result in costly, inequitable, or unconstitutional results. This article will attempt to explore some of these issues from the perspective of the daily practice of law. In resolving disputes through trial or settlement, lawyers and courts are faced with not only the practical application of law to fact, but also broad policy considerations.

Lastly, I undertake this task with a sense of timidity because my knowledge of both the language and mechanics of computers, cell phones, and a host of other digital devices, is limited by both age and education.

II. ELECTRONIC DATA: A PRIMER

Electronic data includes information stored in electronic form that can be produced or restored through the application of programs or software specifically designed to input, store, transmit,

interpret, and reproduce information or data in either electronic or print media. It may include the information specifically requested, the hard drive of a computer, a floppy disk, or a compact disk. Electronic data generally cannot be read or deciphered without the use and application of a software program specifically designed to read or interpret such data. The software program used to recapture or restore such data or the identity of such a program may, therefore, be discoverable. The best evidence of stored data in electronic form is found in the medium used for storage.

The General Assembly provided a definitional source of computer terms.[1] These terms include: computer; computer data; computer network; computer program; computer services; computer software; and electronic mail service provider.[2] The statutory definitions, however, are not as clear as they may appear. For example, a defendant was convicted by the Virginia Beach City Circuit Court under Virginia Code section 18.2-178 for obtaining a computer software package by false pretense, with intent to defraud, when she paid for the item with an uncollectible check.[3] The defendant appealed her conviction, arguing that the set of specifications the company delivered, which could be used to develop a computer program, did not, as charged in the indictment, constitute computer software or a computer program under Virginia Code section 18.2-152.2.[4]

The Court of Appeals of Virginia overturned the defendant's conviction,[5] holding that the specifications were neither a computer program, that is, "an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations;"[6] or computer software defined as a "set of computer programs, procedures and associated documentation concerned with computer data . . . ."[7] The court reasoned that while the specifications described a computer program that could be created, it was not currently in a form that could be executed by a computer, or

1. VA. CODE ANN. § 18.2-152.2 (Cum. Supp. 2007).
2. *Id.*
3. O'Connor v. Commonwealth, 16 Va. App. 416, 417, 430 S.E.2d 567, 567–68 (Ct. App. 1993).
4. *See id.*
5. *Id.* at 418, 430 S.E.2d at 568.
6. VA. CODE ANN. § 18.2-152.2 (Cum. Supp. 2007).
7. *Id.*

cause a computer to perform an operation, and did not relate to an actual computer program in existence.[8]

III. JURISDICTION

Our inquiry begins with the keystone of dispute resolution—personal jurisdiction. Given the universal nature of electronic communications, the practitioner might first ask, can my client be heard in a Virginia court on an issue dealing with electronic data? Under familiar principles, for a court in the Commonwealth to exercise personal jurisdiction over a non-resident defendant, the plaintiff must demonstrate that his allegations fall within the Virginia Long-Arm Statute[9] and that his cause meets the "minimum contacts" requirements of the Due Process Clause of the Fourteenth Amendment.[10]

In *Krantz v. Air Line Pilots Ass'n, Int'l* the court found jurisdiction where a claim by a non-resident for tortious interference with a contract was predicated upon a defendant, a non-resident member of a labor organization located in Virginia, posting information on a computer bulletin board maintained by the organization.[11] The defendant's union placed the plaintiff's name on a "scab list" after he withdrew from an airline pilots' strike.[12] After learning the plaintiff had a successful job interview with another airline, the defendant recorded a message, on his own personal computer in New York, indicating that the plaintiff was a "scab."[13] The defendant then transmitted the message over an electronic switchboard system, operated by the union from its headquarters in Virginia, to union members employed at the other airline.[14]

The Supreme Court of Virginia considered the two-pronged analysis in finding that the plaintiff had established jurisdiction to pursue his claim in the Commonwealth by first addressing the

8. *O'Connor*, 16 Va. App. at 418, 430 S.E.2d at 568.
9. VA. CODE ANN. § 8.01-328.1 (Repl. Vol. 2007).
10. Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).
11. 245 Va. 202, 202–207, 427 S.E.2d 326, 326–29 (1993).
12. *Id.* at 204, 427 S.E.2d at 327.
13. *Id.*
14. *Id.* at 204–05, 427 S.E.2d at 327.

application of the Long-Arm Statute to the facts.[15] The court examined whether the defendant had engaged in some "purposeful activity in Virginia," and whether the result to be obtained was governed by prior case law indicating that fraudulent or defamatory statements made outside the forum state and then transmitted by telephone or mail were not "acts" within the forum jurisdiction.[16] Ultimately, the court determined that the defendant's tortious interference was only completed through the specific use of the computer system operated within the Commonwealth and the subsequent acts of union members who received his message regarding the plaintiff.[17] The court reasoned that without the use of the computer switchboard in Virginia, the defendant could not have obtained the assistance of others, which was necessary to establish an element of tortious interference.[18] The court chose not to decide whether the prior case law correctly limited the applicability of long-arm statutes, so as not to include telephone or mail contacts, because the subsequent acts required to complete the tortious interference in this case rendered those cases inapplicable.[19]

Addressing the Due Process prong of the jurisdictional analysis, the court held that the defendant engaged in purposeful activity through his use of the computer system operated within the Commonwealth and the defendant had the minimum contacts necessary for the plaintiff to maintain his action so that the action did not "offend 'traditional notions of fair play and substantial justice.'"[20]

As early as 1980, the Supreme Court of the United States observed that the limitations imposed by the Due Process Clause on state long-arm statutes had been significantly relaxed due to "a fundamental transformation in the American economy."[21] The pervasive use of the Internet in both personal and business transactions has further transformed our economy and allows an

15. *See id.* at 205–07, 427 S.E.2d at 328–29.

16. *Id.* at 205–06, 427 S.E.2d at 328–29.

17. *See id.* at 206, 427 S.E.2d at 328.

18. *Id.*

19. *Id.*

20. *Id.* at 207, 427 S.E.2d at 328–29; *see* VA. CODE ANN. § 8.01-328.1(B) (Repl. Vol. 2006) ("Using a computer or computer network located in the Commonwealth shall constitute an act in the Commonwealth.").

21. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 292–93 (1980).

online act within one state to have ramifications far beyond those implicated in a long-distance telephone call, or the mailing of a letter to a recipient in another state.

Virginia practitioners should be advised of the varied subsequent impacts of an Internet posting or activity conducted physically in one location, but with the assistance of a computer system operated elsewhere. While the case law and Code of Virginia are clear regarding the specific use of computer systems located within the Commonwealth,[22] current decisions regarding Internet postings are less clear.

In 2002, the United States District Court for the Eastern District of Virginia, in *Verizon Online Services, Inc. v. Ralsky*, found personal jurisdiction based upon Internet use where the defendants reasonably should have expected to be subject to Virginia courts because they were "deliberately exploiting" Verizon's e-mail services for financial gain by transmitting millions of unsolicited bulk e-mails to the plaintiff through the Internet Service Provider ("ISP") located in Virginia.[23] The court cited *Bochan v. La Fontaine* in reaching its decision on jurisdiction.[24] The court in *Bochan* noted that Virginia courts commonly premise the exercise of personal jurisdiction based upon Internet activity by examining both the nature and quality of the activity.[25] Generally, courts determine whether e-mail has been sent for pecuniary gain rather than personal purposes, and in the case of the former the courts find personal jurisdiction.[26]

In 1999, the Loudoun County Circuit Court was confronted with a defamation action commenced in Virginia in which the plaintiff, a Pennsylvania judge, asserted that an unknown individual had published defamatory material on a website located on America Online, an ISP with its principal place of business in Loudoun County, Virginia.[27] The plaintiff caused a subpoena duces tecum to be issued from the clerk of the circuit court requiring the service provider produce documents identifying the individual who owned the website because no service of process could

22. *See, e.g.*, VA. CODE ANN. § 8.01-328.1(B) (Repl. Vol. 2007).
23. 203 F. Supp. 2d 601, 616 (E.D. Va. 2002).
24. *Id.* (citing Bochan v. La Fontaine, 68 Supp. 2d 692, 701 (E.D. Va. 1999)).
25. *See Bochan*, 68 F. Supp. 2d at 701; *see also Ralsky*, 203 F. Supp. 2d at 616.
26. *Ralsky*, 203 F. Supp. 2d at 616.
27. Melvin v. Doe, 49 Va. Cir. 257, 257 (Cir. Ct. 1999) (Loudoun County).

be effected on the defendant in Virginia.[28] The defendant then challenged the jurisdiction of the court by motion and special appearance.[29] In determining whether it had jurisdiction, the court considered whether the allegations could be reconciled with the Virginia Long-Arm Statute.[30] Relying in part on *Krantz*, the court found the allegations sufficient to establish a prima facie showing for the exercise of jurisdiction under the statute because the service provider's server was located within the Commonwealth and because the server's operation was integral to publication.[31] Therefore, the pleading stated a tortious injury caused by an act or omission in the Commonwealth sufficient to satisfy the requirements of Virginia Code section 8.01-328.1(A)(3).[32]

The trial court, however, did not find the facts, as pled, sufficient to satisfy the second prong of the jurisdictional analysis—the "minimum contacts" requirement.[33] The Internet posting in question did not specifically target a Virginia audience and the plaintiff did not allege that the defendant lives, works, or maintains any personal or business relationships in the Commonwealth.[34] To the contrary, the pleadings established a matter of local interest that before the creation of the Internet would only have been published in print by peradventure in the Commonwealth.[35] Accordingly, without prejudice to proceeding in a proper forum, the case was dismissed.[36] Here, the ISP's location as a place for passive, non-commercial postings was not enough to satisfy the "minimum contacts" requirement.[37]

As will be seen, the Virginia General Assembly has been a powerful voice in adapting new technologies to existing law. In 2000, the General Assembly enacted the Uniform Computer Information Transactions Act ("UCITA") governing computer information transactions.[38] The legislature also added section 8.01-

28. *Id.*
29. *Id.*
30. *Id.* at 258.
31. *Id.*
32. *Id.* (quoting Bochan v. La Fontaine, 68 F. Supp. 2d 692, 699 (E.D. Va. 1999)).
33. *Id.*
34. *Id.* at 259.
35. *See id.*
36. *See id.*
37. *See id.*
38. Act. of Apr. 9, 2000, ch. 996, 2000 Va. Acts 2228 (codified at VA. CODE ANN. §§ 59.1-501 to 509.2 (Repl. Vol. 2006)); J. Douglas Cuthbertson & Glen L. Gross, *Annual Sur-*

407.1 to the Virginia Code, providing a helpful and detailed procedure for obtaining subscriber information from ISPs in civil actions "where it is alleged that an anonymous individual has engaged in tortious Internet communications."[39] In such cases, the practitioner confronted with such an issue should be aware of time-sensitive deadlines for making requests, including the requirement that a subpoena and supporting material must be filed with the court at least thirty days prior to the date disclosure is sought.[40]

The Supreme Court of Virginia, by its decision in *America Online, Inc. v. Nam Tai Electronics*, gave guidance for a practitioner seeking discovery of the identity of Internet correspondents.[41] In *Nam Tai*, the plaintiff corporation brought an action for libel and unfair business practices in California arising from certain postings on an Internet message board involving publicly

---

vey of Virginia Law: Technology Law, 37 U. RICH L. REV. 341, 341 (2002).

39. Cuthbertson & Gross, *supra* note 38, at 353.

40. For example, Virginia Code provides:

> At least thirty days prior to the date on which disclosure is sought, a party seeking information identifying an anonymous communicator shall file with the appropriate circuit court a complete copy of the subpoena and all items annexed or incorporated therein, along with supporting material showing:
>
> a. That one or more communications that are or may be tortious or illegal have been made by the anonymous communicator, or that the party requesting the subpoena has a legitimate, good faith basis to contend that such party is the victim of conduct actionable in the jurisdiction where the suit was filed. A copy of the communications that are the subject of the action or subpoena shall be submitted.
>
> b. That other reasonable efforts to identify the anonymous communicator have proven fruitless.
>
> c. That the identity of the anonymous communicator is important, is centrally needed to advance the claim, relates to a core claim or defense, or is directly and materially relevant to that claim or defense.
>
> d. That no motion to dismiss, motion for judgment on the pleadings, or judgment as a matter of law, demurrer or summary judgment-type motion challenging the viability of the lawsuit of the underlying plaintiff is pending. The pendency of such a motion may be considered by the court in determining whether to enforce, suspend or strike the proposed disclosure obligation under the subpoena.
>
> e. That the individuals or entities to whom the subpoena is addressed are likely to have responsive information.
>
> f. If the subpoena sought relates to an action pending in another jurisdiction, the application shall contain a copy of the pleadings in such action, along with the mandate, writ or commission of the court where the action is pending that authorizes the discovery of the information sought in the Commonwealth.

VA. CODE ANN. § 8.01-407.1(A)(1) (Repl. Vol. 2007).

41. 264 Va. 583, 590–95, 571 S.E.2d 128, 132–35 (2002).

traded stock in the corporation.[42] Pursuant to a commission issued by the California court, a subpoena duces tecum was issued directing the ISP to produce subscriber information relating to the author of a posting made under an anonymous screen name.[43] The ISP, with corporate offices located in Loudoun County, Virginia, filed a motion to quash on behalf of its anonymous subscriber.[44] The Supreme Court of Virginia affirmed the decision of the trial court that declined America Online's request to quash the subpoena.[45] Interestingly, the Virginia court requested a clarifying order from the California court prior to deciding the motion.[46] In so doing, the Supreme Court of Virginia noted the similarities between the procedures governing such motions in California and Virginia.[47]

IV. DISCOVERY

In preparation for both civil and criminal trials, a lawyer may be required to take steps that are directly related to electronic data. Thus, he or she may be called upon to preserve, acquire, catalogue, or protect electronic data. As part of the pretrial discovery process, it may be necessary to identify electronic data and to prepare suitable responses to specific discovery requests.

Discovery may include depositions, written interrogatories, requests for admissions, and subpoenas to third parties. Before a response can be initiated or a request tailored to the issues presented in a case, it is important to identify what data is requested, in what form it is kept, and how it is relevant to the issues presented by the underlying action. The Rules of the Supreme Court of Virginia provide:

---

42. *See id.* at 586, 571 S.E.2d at 129.

43. *See id.* at 587–88, 571 S.E.2d at 130.

44. *Id.*

45. *Id.* at 596, 571 S.E.2d at 135.

46. *Id.* at 589, 571 S.E.2d at 131.

47. *See id.* at 591, 571 S.E.2d at 132; *see also* America Online, Inc. v. Anonymous Publicly Traded Co., 261 Va. 350, 360, 542 S.E.2d 377, 383 (2001) ("Virginia courts should grant comity to any order of a foreign court of competent jurisdiction, entered in accordance with the procedural and substantive law prevailing in its judicatory domain, when that law, in terms of moral standards, societal values, personal rights, and public policy, is reasonably comparable to that of Virginia." (quoting Oehl v. Oehl, 221 Va. 618, 623, 272 S.E.2d 441, 444 (1980))).

> Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter.[48]

Practitioners must take care in assessing the importance of moving for discovery of such data because it may be both costly and time consuming. When relevant to the issues, however, no more powerful evidence can be obtained. The strength of such evidence comes from the neutrality of the third parties involved in the obtaining and retention of such data; such as telecommunications carriers, cable companies, and ISPs.

In seeking electronic data, a host of issues may arise that are unfamiliar to the practitioner who was raised on "paper discovery." Notice is an important consideration in evaluating a search for such data. For example, ISPs are required to notify subscribers of requests for subscribers' information, and the ISPs may assert privilege claims on their behalf.[49] Requesting parties may wish to employ experts, when necessary, and be prepared to adhere to protective orders limiting access and the use of the materials. Deleted data may be recaptured or restored later, unlike a paper placed in the trash for delivery to the dump. Deleted data will likely be the first thing sought and the last thing a party may want to produce.

Ownership of a computer does not automatically grant access to matters otherwise privileged. A test that could be applied in the case of a computer owned by another or subject to use by more than one person is whether the creator or user of such information had an expectation of privacy in the communications made or kept; or whether the use of the computer was for an employer or for company business.

Factors to consider in the protection of such data from disclosure would be the nature of the data transmitted, the authority of the person accessing the data, and the expectation of privacy of the person involved in the communication. Discovery requests should be carefully tailored to avoid being attacked as overreach-

48. VA. SUP. CT. R. 4:1.

49. *See* VA. CODE ANN. § 8.01-407.1(A)(3)–(4) (Repl. Vol. 2007).

ing. Specific requests must only consist of data that is relevant to the subject matter involved in the underlying action.[50] This may include a request for the identification of the place where the data is stored, the production of a hard drive, compact disk or floppy disk, as well as the identification of, or access to, the application software necessary to access the data.

Impediments to production may include such issues as: relevancy and materiality; privilege; adherence to procedural guidelines; record keeping and capture; over-reaching (burdensome discovery); spoliation; duplication; authentication; interpretation; and the need for expert assistance.[51] The Rules of the Supreme Court of Virginia require the production of data compilations in a reasonably useable form, including material translated by detection devices.[52] Therefore, electronic data compilations are "documents" that are subject to production.[53] The fact that computers may contain encrypted information does not appear to limit access because the information could be obtained, albeit with greater difficulty. It is best to request both printed and electronic versions.

Any claim of privilege regarding electronic data must include a privilege list, known in practice as a "Vaughn Index."[54] In developing a privilege list, the separation of privileged material from that which is not privileged may prove difficult when the disputed material is contained in computer storage. For instance, personal privileged e-mail may be stored on a company computer. Where a company permits the use of its computer for personal use, such material may remain recoverable even after the employee has ceased work with the business and turned in the computer. Employers should be advised with respect to such issues, and employees should be reminded of the nature of e-mail transmissions and the manner in which they are kept and retained.

Interesting issues arise when evaluating discovery requests and privilege claims related to electronic communications transmitted through ISPs. If a privilege claim is asserted or contested,

---

50. *See* VA. SUP. CT. R. 4:1.

51. *See id.*

52. VA. SUP. CT. R. 4:9.

53. *See id.*

54. *See* VA. SUP. CT. R. 4:1(b)(6); *see generally* Vaughn v. Rosen, 484 F.2d 820, 827–28 (D.C. Cir. 1973) (setting forth indexing requirement) .

factors to consider might include: agreements between individuals and communications carriers such as ISPs; access to passwords necessary to unlock the stored data; past use of the storage medium; and agreements between the owner and user. E-mail content can be accessed by the ISP, and data deleted from the hard drive of the sending or receiving computer may still be accessed on a server. Additionally, information retained by Internet companies may be recovered by subpoena or court order.

There is a difference, however, between stored and intercepted electronic data. An oral communication is protected where the speaker expects the conversation not to be intercepted and circumstances justify that belief.[55] E-mail may likewise be privileged where the author has a reasonable expectation of privacy in such communication, even though the e-mail is subject to inspection by an ISP or employer. Encryption, although unnecessary to invoke the privilege, does heighten the level of security in the conversation or transmission. Ownership of the storage medium and the expectation of privacy in retaining data in the storage medium serve as guideposts for Virginia courts in deciding claims of privilege. For example, the right to correspond anonymously is protected by the First Amendment,[56] and the Internet has been recognized as a significant medium of communication subject to ordinary First Amendment scrutiny.[57] Furthermore, an ISP has standing to assert some rights of its anonymous subscribers.[58]

The attorney-client privilege and the work product doctrine play an important role in the discovery and use of electronic data if the claim extends to electronic documents prepared by the attorney or supporting staff,[59] or even electronic documents prepared by the client with the intention of securing legal advice on its contents.[60] Electronic communications between officers and

55. Wilks v. Commonwealth, 217 Va. 885, 888, 234 S.E.2d 250, 252 (1977) (wiretap interception).

56. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995).

57. *See* Reno v. ACLU, 521 U.S. 844, 850, 870 (1997) (ruling that Internet speech is protected by the same level of First Amendment scrutiny as other media).

58. *See, e.g.*, NAACP v. Alabama, 357 U.S. 449, 459–60 (1958) (noting that effect on organization is considered where lists of members sought in discovery).

59. *See* Commonwealth v. Edwards, 235 Va. 499, 509–10, 370 S.E.2d 296, 301–02 (1988) (citing Hickman v. Taylor, 329 U.S. 495, 511 (1947)).

60. *See* Va. Elec. & Power Co. v. Westmoreland-LG&E Partners, 259 Va. 319, 325, 526 S.E.2d 750, 755 (2000) (citing Robertson v. Commonwealth, 181 Va. 520, 539–40, 25 S.E.2d 352, 360 (1943)).

employees of the same entity relayed to corporate counsel for obtaining legal advice are also entitled to the attorney-client privilege.[61] Electronic materials prepared in anticipation of litigation (i.e., work product) are shielded from discovery just like their tangible equivalents, absent a showing of substantial need and undue hardship in obtaining the substantial equivalent of such materials by other means.[62]

Some courts have used a test, as equally applicable to electronic evidence as to other evidence, to determine if materials are considered work product because litigation was reasonably foreseeable at the time the materials were prepared.[63] Once the party asserting privilege meets the burden of demonstrating that the materials in question were prepared in anticipation of litigation, the opposing party must prove a substantial need for the information and the inability to otherwise acquire the materials without undue hardship.[64]

In *Malone v. Ford Motor Co.*, the defendant corporation contended that a computerized database used to manage information, including documents furnished separately in discovery, was work product because counsel assisted in the development and updating of the database in anticipation of litigation.[65] The court held that the database was work product and reasoned that "[t]he mere possibility that a party might not produce all relevant, unprotected documents, is not a sufficient basis for ordering such a party to disclose its entire computerized system of information management."[66] As rapid technological change continues, varied degrees of capability in taking advantage of technology are inevitable between adverse parties. The court must strike a balance in assessing undue burden claims, respecting the technological abilities of the parties while preventing a perverse incentive to argue lack of technological capabilities in order to avoid electronic discovery requests.

---

61. *Id.* at 326, 526 S.E.2d at 755 (citing Owens-Corning Fiberglass Corp. v. Watson, 243 Va. 128, 141, 413 S.E.2d 630, 638 (1992)).

62. VA. SUP. CT. R. 4:1(b)(3); *see generally Hickman*, 329 U.S. at 512 (establishing burden to overcome work product protection).

63. *See, e.g.*, Larson v. McGuire, 42 Va. Cir. 40, 42–43 (Cir. Ct. 1997) (Loudoun County).

64. *See id.* at 43.

65. 29 Va. Cir. 456, 456–57 (Cir. Ct. 1992) (Loudoun County).

66. *Id.* at 459 (quoting Lawyers Title Ins. Corp. v. U.S. Fid. & Guar. Co., 122 F.R.D. 567, 570 (N.D. Cal. 1988)).

During the pretrial phase of litigation, Virginia practitioners should work with their clients to ensure electronic data subject to discovery is maintained because spoliation of electronic evidence may merit sanctions if bad faith or prejudice can be proven.[67] In *Gentry v. Toyota Motor Corp.*, an expert employed by the plaintiff's attorney removed a part from a car involved in an auto accident without authorization or permission.[68] The Supreme Court of Virginia ruled that the trial court had abused its discretion when dismissing the case because there was no evidence of bad faith on the part of the plaintiff, who had not authorized the expert's actions.[69] When considering claims of the destruction of evidence it is important to note that there is no independent cause of action for spoliation of evidence in Virginia.[70]

V. EVIDENTIARY ISSUES

Once the pretrial phase is complete, attention focuses on the trial. In preparing for trial, the lawyer should be mindful of evidentiary issues that may arise to ensure admission of critical pieces of evidence. This would, in most cases, involve the harmonizing of data collection and storage techniques with traditional rules of evidence. A review of extant case authority reveals the extent to which traditional rules of evidence may be applied to the use of electronic data.

The admission of electronic evidence is controlled by common law and statutory proscription. Where there exists a possibility of contamination of evidence, the proponent of the exhibit must demonstrate to a reasonable certainty that the evidence has not been tampered with.[71] The reasonable certainty requirement, however, is not met if a "vital link in the chain of possession is not accounted for. . . ."[72]

---

67. *See, e.g.*, Gentry v. Toyota Motor Corp., 252 Va. 30, 34, 471 S.E.2d 485, 488 (1996).

68. *Id.*, 471 S.E.2d at 486 (1996).

69. *Id.*, 471 S.E.2d at 488. Additionally, the underlying theory of the case ultimately rested on another part in the car that had not been damaged. *Id.*

70. *See* Austin v. Consolidation Coal Co., 256 Va. 78, 83–84, 501 S.E.2d 161, 163–64 (1998).

71. Robinson v. Commonwealth, 212 Va. 136, 138, 183 S.E.2d 179, 180 (1971).

72. *Id.*

The admission of computer data that represents material gathered by persons rather than gathered in response to electronic stimuli is governed by the business records exception to the hearsay rule.[73] The reliability of electronic data is controlled by familiar principles. Where the reliability of data generated by a computer is dependent on proof of scientific accuracy, however, expert testimony may be required. For example, information gathered by a "call trap" placed on a telephone to record calls to a residence requires a showing of reliability.[74]

In *Penny v. Commonwealth*, the Court of Appeals of Virginia held that once the reliability of a call trap device has been proven, the results attendant to its use may be received into evidence.[75] The court in *Penny*, however, made clear that the "requirement of proof of reliability for each call trap may not necessarily apply to other instances involving computer generated data."[76] Because the call trap is generally utilized for litigation purposes in an adversarial process "of ferreting out criminal agents," the court reasoned an additional check for reliability is necessary.[77] The court reasoned that call trap evidence is just the recording of electronic events without human interaction.[78] Therefore, hearsay concerns are unfounded as no out-of-court declarant exists who could be subject to cross-examination.[79]

In *Tatum v. Commonwealth*, the Court of Appeals of Virginia found that "caller ID" data is also not hearsay because it is based on computer generated information and is not a record of human input and observation.[80]

Call trap and caller ID evidence of telephone communications are treated differently than computer recordings of the content of conversation.[81] Under Virginia Code section 8.01-420.2, "[n]o me-

73. *See* Frye v. Commonwealth, 231 Va. 370, 387, 345 S.E.2d 267, 279–80 (1986) (finding the business records exception to the hearsay rule applies to computer printout from the National Crime Information Center).

74. Penny v. Commonwealth, 6 Va. App. 494, 499, 370 S.E.2d 314, 317 (Ct. App. 1988).

75. *Id.*

76. *Id.* at 500 n.3, 370 S.E.2d at 317 n.3.

77. *Id.*

78. *Id.* at 498, 370 S.E.2d at 317.

79. *See id.*

80. 17 Va. App. 585, 588, 440 S.E.2d 133, 135 (Ct. App. 1994).

81. *See, e.g.*, VA. CODE ANN. § 8.01-420.2 (Repl. Vol. 2000) (limitations on admissibility in civil proceedings of recordings of telephone conversations).

chanical recording, electronic or otherwise, of a telephone conversation" can be admitted into evidence in any civil proceeding unless all parties to the conversation are aware they are being recorded and certain other conditions are met.[82] Under Virginia Code section 19.2-61(b), an oral communication intercepted electronically is also protected where the speaker expects the conversation not to be intercepted and the circumstances justify that belief.[83] The constitutional expectation of privacy under the Fourth Amendment is applied in such circumstances.[84] The contents of an intercepted communication and the evidence derived from such communications (both wire and oral) may be subject to suppression in both criminal and civil cases.[85]

Individuals often identify themselves online using screen names or e-mail addresses which complicates the process of identification. The Supreme Court of Virginia ruled that the identity of an individual corresponding over the Internet can be established at trial by direct or circumstantial evidence such as e-mail or participation in group discussions such as "chat rooms."[86] In *Bloom v. Commonwealth*, the statements made over the Internet by a defendant were properly admitted into evidence under the party admission exception to the hearsay rule.[87] The measure of proof necessary to establish identity and for the admission of such evidence is by a preponderance of the evidence.[88] In *Bloom*, however, the Supreme Court of Virginia explicitly chose not to adopt the trial court's assertion that conversations over the Internet are analogous to conversations over the telephone reasoning that the

82. *Id.* Specifically, "all parties to the conversation were aware the conversation was being recorded or (ii) the portion of the recording to be admitted contains admissions that, if true, would constitute criminal conduct which is the basis for the civil action, and one of the parties was aware of the recording and the proceeding is not one for divorce, separate maintenance or annulment of a marriage. The parties' knowledge of the recording pursuant to clause (i) shall be demonstrated by a declaration at the beginning of the recorded portion of the conversation to be admitted into evidence that the conversation is being recorded. This section shall not apply to emergency reporting systems operated by police and fire departments and by rescue squads, nor to any communications common carrier utilizing service observing or random monitoring pursuant to § 19.2-62." *Id.*

83. VA. CODE ANN. § 19.2-61(b) (Cum. Supp. 2007); *see generally* Wilks v. Commonwealth, 217 Va. 885, 888, 234 S.E.2d 250, 252 (1977).

84. *See Wilks*, 217 Va. at 888–89, 234 S.E.2d at 252.

85. VA. CODE ANN. § 19.2-65 (Repl. Vol. 2004).

86. *See* Bloom v. Commonwealth, 262 Va. 814, 820–21, 554 S.E.2d 84, 87 (2001).

87. *Id.* at 820, 554 S.E.2d at 87.

88. *Id.* at 821, 554 S.E.2d at 87 (citing Witt v. Commonwealth, 215 Va. 670, 674, 212 S.E.2d 293, 296 (1975)).

parties do not have the opportunity for voice recognition during Internet communications.[89]

VI. CRIMINAL PROSECUTIONS

In addition to civil liability arising from actions performed with computers, and the issues that arise from the use of computers and electronic records in the litigation process, computers may be used in the commission of crimes. Criminal proscriptions that traditionally existed without the use of electronic media have been extended into the digital world. For instance, the alteration of public computer records has been held to constitute forgery despite the absence of a traditional writing on paper.[90] Computer activities may also be used as evidentiary support for traditional crimes.[91]

Crimes specifically arising from the possession and use of computers and computer networks have been identified by the General Assembly in the Virginia Computer Crimes Act ("VCCA").[92] The Act does not explicitly preclude prosecution under other statutes for crimes that may also fall under the VCCA unless clearly inconsistent with the terms of the Act.[93] The VCCA reflects a continued understanding of the importance of technology in society while balancing the need to protect citizens from the pervasive impact of global computer networks that reach into our homes and businesses.

The VCCA makes it a crime to fraudulently use a computer to obtain property, including money.[94] This prohibition has been read broadly to include activities in furtherance of a theft, such as checking vehicle identification numbers ("VIN") through the

89. *Id.* at 822 n.2, 554 S.E.2d at 88 n.2.

90. *See* Campbell v. Commonwealth, 246 Va. 174, 176–78, 431 S.E.2d 648, 649–51 (1993).

91. *See* Barnes v. Commonwealth, No. 2693-98-1, 2000 Va. App. LEXIS 204 (Ct. App. Mar. 21, 2000) (unpublished decision). In *Barnes*, evidence of computer searches of a stolen vehicle database were used to show that a police officer was aware that property she received was stolen. *Id.* at *4–6.

92. Act of Apr. 11, 1984, ch. 751, 1984 Va. Acts 1759 (codified as amended at VA. CODE ANN. §§ 18.2-152.1 to -.15 (Repl. Vol. 2004 & Cum. Supp. 2007)).

93. VA. CODE ANN. § 18.2-152.11 (Repl. Vol. 2004).

94. *Id.* § 18.2-152.3 (Cum. Supp. 2007).

Commonwealth computer network to ascertain whether a vehicle remained on a list of stolen vehicles.[95]

The VCCA also makes it a crime to send spam e-mail, called "Unsolicited Bulk Email" ("UBE") under certain circumstances.[96] Falsifying the transmission information or trafficking in software designed to falsify that information is a misdemeanor.[97] Sending bulk e-mail to more than a certain number of intended recipients or bulk e-mail that generates more than a certain amount of revenue constitutes a class six felony.[98] Additionally, the employment of a minor to violate the proscriptions on bulk e-mail is a felony.[99] The VCCA also creates civil liability for sending unsolicited bulk e-mail, including significant statutory damages.[100]

A prosecution for a violation of the Virginia spam statute resulted in a challenge based upon, among other things, constitutional Due Process, Free Speech, and Commerce Clause violations.[101] While the trial court's conviction was affirmed by the court of appeals,[102] the matter is currently on appeal to the Supreme Court of Virginia.[103]

Computer trespass is defined to include a myriad of activities that interfere with the normal functioning of a computer, or using a computer or network to make unauthorized copies of data or software.[104] Computer trespass is a class one misdemeanor unless the trespass causes damage to another's property in excess of

95. *Barnes*, 2000 Va. App. LEXIS 204, at *4–6.

96. VA. CODE ANN. § 18.2-152.3:1 (Repl. Vol. 2004 & Cum. Supp. 2007).

97. *Id.* § 18.2-152.3:1(A)(2)(ii)–(iii) (Repl. Vol. 2004 & Cum. Supp. 2007). Federal law now supersedes most state anti-spam laws except for those like Virginia's that prohibit falsity or deceit in any portion of an electronic mail message or attachments thereto. 15 U.S.C. § 7707(b)(1) (Supp. 2007).

98. VA. CODE ANN. § 18.2-152.3:1(B) (Repl. Vol. 2004 & Cum. Supp. 2007). The number of recipients is 10,000 recipients in a day, 100,000 within 30 days, or 1,000,000 in a year; the revenue is $1,000 for a specific transmission or $50,000 from the customers of any individual mail provider. *Id.*

99. *Id.* § 18.2-152.3:1(C) (Repl. Vol. 2004 & Cum. Supp. 2007).

100. *Id.* § 18.2-152.12(B)–(C) (Cum. Supp. 2007). If requested, courts have the ability to protect the secrecy and security of parties engaged in litigation that arises out of the VCCA. *Id.* § 18.2-152.12(D) (Cum. Supp. 2007).

101. *See* Commonwealth v. Jaynes, 65 Va. Cir. 355, 357, 363, 365–67 (Cir. Ct. 2004) (Loudoun County).

102. Jaynes v. Commonwealth, 48 Va. App. 673, 704, 634 S.E.2d 357, 372 (Ct. App. 2006) (appeal docketed), No. 062388 (Va. Apr. 24, 2007).

103. *See* Supreme Court of Virginia Appeals Docketed, http://www.courts.state.va.us/scv/appeals/062388.html (last visited Sept. 17, 2007).

104. *See* VA. CODE ANN. § 18.2-152.4(A) (Cum. Supp. 2007).

$1,000, in which case it is a class six felony.[105] The section of the statute proscribing computer trespass explicitly does not apply to Virginia ISPs' e-mail filtering activities or to parental monitoring.[106] It also explicitly allows parties to contract around the proscription.[107] The VCCA also creates civil liability for computer trespass regardless of malice.[108]

Recognizing the power of computers and networks to access a great deal of information, the Virginia General Assembly created a protection against invasion of privacy using computers.[109] The VCCA makes it a class one misdemeanor to use a computer or network to examine personal information, such as financial, employment, or identifying information about another person without permission.[110] The violation is upgraded to a class six felony if the perpetrator then sells or distributes the information, commits the violation in the course of committing another crime, or has previously been found guilty of the same act or a substantially similar crime in the United States.[111] There is an exception for persons collecting information that is reasonably needed for computer security, for diagnostics or repair, or for purposes of identifying a computer user.[112] Although the statute requires that the person know he is without authority at the time the information is examined,[113] the statute has been interpreted broadly.[114] Theft

105. *Id.* § 18.2-152.4(B) (Cum. Supp. 2007).

106. *See id.* § 18.2-152.4(C) (Cum. Supp. 2007).

107. *Id.*

108. *Id.* § 18.2-152.12(A) (Cum. Supp. 2007). The statute of limitations for actions arising out of this section are contained in section 18.2-152.12(F). If requested, courts have the ability to protect the secrecy and security of parties engaged in litigation that arises out of the VCCA. *Id.* § 18.2-152.12(D) (Cum. Supp. 2007).

109. Act of Apr. 11, 1984, ch. 751, 1984 Va. Acts 1759 (codified as amended at VA. CODE ANN. § 18.2-152.5 (Cum. Supp. 2007)).

110. *See* VA. CODE ANN. § 18.2-152.5(A)–(B) (Cum. Supp. 2007).

111. *See id.* § 18.2-152.5(C)–(E) (Cum. Supp. 2007).

112. *See id.* § 18.2-152.5(F) (Cum. Supp. 2007).

113. *See id.* § 18.2-152.5(A) (Cum. Supp. 2007).

114. *See, e.g.*, Plasters v. Commonwealth, No. 1870-99-3, 2000 Va. App. LEXIS 473 (Ct. App. June 27, 2000) (unpublished decision) (decided under prior statute). In *Plasters*, a dispatcher accessed personal information that was contained in the Virginia Criminal Information Network while working as a police dispatcher. *Id.* at *2–3. The court of appeals held that it did not matter the defendant did not know that accessing the personal information was a crime, and it affirmed the defendant's convictions because of an on-screen warning that information from the system was to be used for criminal justice purposes only. *Id.* at *5–6. *Plasters* did draw a dissent, which noted that the handbook the employee received did not contain an admonition against viewing the type of information involved, while the release of other information was clearly defined as unauthorized by the hand-

of computer services is also a misdemeanor under the VCCA, or a felony if the value of services stolen is over $2,500.[115]

The VCCA defines the crime of personal trespass by computer as the use of a computer or computer network to cause physical injury to an individual.[116] This is a class six felony if committed unlawfully but not maliciously, and a class three felony if done maliciously.[117] Malice in this circumstance is defined in accordance with familiar principles as the state of mind that results in the completion of a wrongful act when the mind is within the control of reason and without justification or legal excuse.[118] There has been at least one attempt to apply personal trespass by computer to injuries to the profitability of a business, but it is not clear that this extension can be maintained.[119]

Harassment by computer is also a crime defined by the VCCA.[120] Harassment is a class 1 misdemeanor, which involves using a computer or network to make one of a variety of obscene or vulgar communications with the intent to harass or intimidate.[121]

In Virginia Code section 18.2-152.8, the legislature provides a laundry list of property subject to embezzlement, including computers, networks, financial instruments, data, software, and all other personal property.[122] The taking of these assets, whether tangible or intangible, in a readable format, or even in transit between devices, is considered embezzlement.[123] The provision also

---

book. *Id.* at *8–9 (Benton, J., dissenting). The overall breadth of the privacy protection may still not be well defined.

115. VA. CODE ANN. § 18.2-152.6 (Cum. Supp. 2007).

116. *Id.* § 18.2-152.7(A) (Cum. Supp. 2007).

117. *Id.* § 18.2-152.7(B) (Cum. Supp. 2007).

118. Saunders v. Commonwealth, 31 Va. App. 321, 324, 523 S.E.2d 509, 510 (Ct. App. 2000).

119. *See* Saks Fifth Ave., Inc. v. James, Ltd., 272 Va. 177, 630 S.E.2d 304 (2006). *Saks* involved a salesperson who switched employment to a competing firm and brought electronic customer records stored on his computer with him; he apparently contacted former customers using e-mail. *Id.* at 182, 630 S.E.2d at 307. *Saks* was a civil dispute, but persons injured by actions taken under *any* section of the Virginia Computer Crimes Act may recover under Virginia Code section 18.2-152.12, which provides for civil actions. VA. CODE ANN. § 18.2-152.12 (Cum. Supp. 2007). However, the trial court struck the evidence as to the claim for conversion based on personal trespass by computer. *See Saks*, 272 Va. at 185 n.11, 630 S.E.2d at 309 n.11.

120. *See* VA. CODE ANN. § 18.2-152.7:1 (Repl. Vol. 2004 & Cum. Supp. 2007).

121. *Id.*

122. *Id.* § 18.2-152.8 (Cum. Supp. 2007).

123. *Id.*

applies to computer services.[124] In *Perk v. Vector Resources Group*, the Supreme Court of Virginia held that the value of information contained in computer files was a matter of fact to be decided at trial.[125] Creating, altering, or deleting computer data in a manner that would constitute forgery on traditional media is deemed to be forgery under the VCCA.[126] The Act also makes it an independent misdemeanor to willfully use encryption in furtherance of any criminal activity.[127]

Computer crimes have not escaped the implications of forfeiture. In Virginia, all computer equipment, software, and other personal property used in a computer crime defined by the VCCA can be subject to forfeiture.[128] There is also a specific statute of limitations provision for crimes arising out of the VCCA—misdemeanors pursuant to the VCCA must be prosecuted within five years of the last act constituting the violation, or one year after the act or identity of the offender was discovered.[129] A criminal prosecution for an act proscribed by the VCCA has a wide choice of venues. Venue may lie where any of the acts in furtherance of the crime were committed, where the owner has a principal place of business, where the offender has control or possession of material used to commit the crime, where access to a computer or network was made, where the offender resides, or where a

124. *Id.* § 18.2-152.8(3) (Cum. Supp. 2007).

125. 253 Va. 310, 315, 485 S.E.2d 140, 143 (1997). *Perk* was a civil case based on the computer crimes act. *Id.* The plaintiff, an attorney who had been hired to collect on the defendant's outstanding debts, claimed that he had invested substantial time and money in creating his own computer programs and databases for the project, and that the defense had converted programs, databases, software, and data in violation of the statute. *Id.* at 313, 485 S.E.2d at 142. The defense claimed that the items allegedly converted were nothing more than the plaintiff's client's lists, that they belonged to the employer and that the lists were of no value to the plaintiff once the contract had been terminated. *Id.* at 315, 485 S.E.2d at 143. The trial court granted a demurrer. *Id.* at 312, 485 S.E.2d at 141–42. The Supreme Court of Virginia held that the question of whether those items had value to the contractor other than his obligations to his employer was a matter of proof that cannot be decided on demurrer. *Id.* at 315, 485 S.E.2d at 143.

126. VA. CODE ANN. § 18.2-152.14 (Repl. Vol. 2004); *see also* Commonwealth v. Bechtler, 56 Va. Cir. 186 (Cir. Ct. 2001) (Rockingham County). In *Bechtler*, this section of the VCCA was held not to extend to copies of the seal on the Virginia driver's license, because the image on the license is not actually the Virginia seal, but a mere representation. *Id.* at 187. Because the statute imputes liability for what would be a crime without a computer, the court dismissed the indictment because the underlying conduct would not be considered a forgery. *Id.*

127. VA. CODE ANN. § 18.2-152.15 (Repl. Vol. 2004).

128. *See* VA. CODE ANN. § 19.2-386.17 (Repl. Vol. 2004).

129. *Id.* § 19.2-8 (Cum. Supp. 2007).

computer that was an instrument or object of the crime was at the time of the commission.[130]

One area of traditional criminal law that is particularly relevant to changing electronic technology is wiretapping. Wiretapping laws were enacted to allow law enforcement officers to respond to a different generation of criminal activity with new and innovative technology. Traditional privacy concerns are reflected in the Interception of Wire, Electronic, or Oral Communications Act ("IWEOCA").[131] The Act has broad applications—defining, for instance, "electronic communication systems" as including computer facilities.[132] The Act makes it a felony to unlawfully:

> i. Intentionally intercept, or procure another to intercept, any wire, electronic, or oral communication;
>
> ii. Intentionally use, or procure another to use, an electronic, mechanical, or other device to intercept an oral communication;
>
> iii. Intentionally disclose the contents of a wire, electronic, or oral communication knowing that it was obtained through an interception of a wire, electronic, or oral communication; or
>
> iv. Intentionally use the contents of a wire, electronic, or oral communication knowing it to have been obtained through interception.[133]

There are, however, exceptions. The exceptions for communications service providers relate primarily to activities arising in the normal course of business or service quality checks, as well as in assistance to law enforcement officers who are authorized to intercept communications.[134] While the statute allows service providers to intercept communications, they are prevented from divulging the contents of any communications.[135] Another exception is made for situations where one of the parties to the communication has consented.[136] Other exceptions are made for communications that are already accessible to the general public and radio

130. *Id.* § 19.2-249.2 (Cum. Supp. 2007).
131. *See id.* §§ 19.2-61 to -70.3 (Repl. Vol. 2004 & Cum. Supp. 2007).
132. *Id.* § 19.2-61 (Cum. Supp. 2007).
133. *Id.* § 19.2-62(A) (Repl. Vol. 2004 & Cum. Supp. 2007).
134. *Id.* § 19.2-62(B)(1), (3)(f) (Repl. Vol. 2004 & Cum. Supp. 2007).
135. *Id.* § 19.2-62(C) (Repl. Vol. 2004 & Cum. Supp. 2007).
136. *Id.* § 19.2-62(B)(2) (Repl. Vol. 2004 & Cum. Supp. 2007).

communications such as those made on emergency, nautical, or amateur frequencies.[137]

Detailed procedures are set forth for court ordered authorization of the interception of wire, electronic, and oral communications.[138] Less stringent procedures are provided in the case of the disclosure of customer and subscriber information, excluding the contents of electronic communication.[139] While electronic communication *transfers* are subject to detailed procedures in the IWEOCA, the contents of e-mail stored with a service provider would be subject to the general requirements for the issuance of a search warrant.[140] Virginia makes good faith reliance by a person upon a court order or legislative authorization a complete defense to an action for unlawful interception, disclosure, or use.[141]

IWEOCA defines "pen registers" and tracing devices separately.[142] A pen register is a device that records dialing, routing, addressing, or signal information transmitted by an instrument (but not the contents of the communication) while a "trap and trace device" captures incoming electronic identifiers.[143] The Act excludes any device used for billing from its pen register definition.[144] Pen registers are banned under the Act, absent a court order, and have different exceptions than those for content-based communications.[145] The Act makes it a class one misdemeanor to use a pen register or trap and trace without a court order.[146] The only exceptions to this are for service providers using the routing information to test or maintain equipment, record the fact that a communication occurred to protect from fraud or abuse of service, or where the user consents.[147]

Evidence from pen registers used at the request of one party to a communication is admissible in criminal proceedings. For in-

137. *Id.* § 19.2-62(B)(3) (Repl. Vol. 2004 & Cum. Supp. 2007).
138. *Id.* § 19.2-68 (Cum. Supp. 2007).
139. *See id.* § 19.2-70.3 (Repl. Vol. 2004).
140. *See id.* § 19.2-53 (Repl. Vol. 2004).
141. *Id.* § 19.2-69 (Repl. Vol. 2004).
142. *Id.* § 19.2-61 (Cum. Supp. 2007).
143. *Id.*
144. *Id.*
145. *Compare id.* § 19.2-70.1 (Repl. Vol. 2004), *with id.* § 19.2-62(B) (Repl. Vol. 2004 & Cum. Supp. 2007).
146. *Id.* § 19.2-70.1 (Repl. Vol. 2004). The statute provides specific regulations for when a court order will be issued in section 19.2-70.2. *Id.* § 19.2-70.2 (Cum. Supp. 2007).
147. *See id.* § 19.2-70.1 (Repl. Vol. 2004).

stance, in *Harmon v. Commonwealth*, the telephone company, at the customer's request, attached a pen register to the phone line where they were receiving obscene telephone calls.[148] The company took this action without police involvement.[149] The Supreme Court of Virginia upheld the trial court's admission of the evidence from the pen register.[150]

The Virginia wiretap laws, like the VCCA, create civil liability for perpetrators.[151] People whose communications are used or disclosed unlawfully in violation of the Act can recover both compensatory and punitive damages, as well as attorney's fees.[152] An oral communication, however, is protected where the speaker expects the conversation not to be intercepted and the circumstances justify that belief.[153] The contents of an intercepted communication and the evidence derived from those communications (both wire and oral) are subject to suppression in both criminal and civil cases.[154]

VII. FEDERAL LESSONS

The revised Federal Rules of Civil Procedure may give some guidance in the treatment of electronic discovery requests. The Federal Rules address the emerging role of electronic data in the discovery process by recognizing that "electronic information must be treated on equal footing with paper documents."[155] Federal Rule of Civil Procedure 34(a) now specifically includes "electronically stored information" as discoverable material in a request for production of documents.[156] The revised Federal Rules now require that if a request for electronically stored information

148. 209 Va. 574, 575–76, 166 S.E.2d 232, 233 (1969). *Harmon* dealt with application of a federal statute that was substantively similar to Virginia law as to the wiretapping issue. For example, see 47 U.S.C. § 605 (2000).

149. *Harmon*, 209 Va. at 577, 166 S.E.2d at 234–35.

150. *Id.* at 579, 166 S.E.2d at 235.

151. VA. CODE ANN. § 19.2-69 (Repl. Vol. 2004).

152. *Id.* § 19.2-69(1)–(3) (Repl. Vol. 2004).

153. *See* Wilks v. Commonwealth, 217 Va. 885, 889, 234 S.E.2d 250, 252.

154. *See* VA. CODE ANN. § 19.2-65 (Repl. Vol. 2004). As has been demonstrated in other jurisdictions, however, information stored on a computer may not be subject to suppression. *See* White v. White, 781 A.2d 85, 87 (N.J. Super. Ct. Ch. Div. 2001).

155. Jason Krause, *E-Discovery Gets Real*, 93 A.B.A. J., Feb. 2007, at 44, 46.

156. FED. R. CIV. P. 34(a). *But cf.* VA. SUP. CT. R. 4:9(a) (no provision for "electronically stored information").

does not specify the form for production, the information is to be produced in the form ordinarily maintained or the form reasonably useable.[157] Additionally, the Federal Rules do not require production in more than one form.[158] The importance of electronic data and the possibility of its unprecedented volume is therefore apparent throughout the pretrial process.

If the Commonwealth adopted similar language regarding the production of electronic databases along with electronic documents themselves, issues such as those addressed in *Malone* could easily be resolved.[159] Federal Rule of Civil Procedure 26(b) was also amended to excuse a party from producing discoverable electronic data if it is not "reasonably accessible because of undue burden or cost."[160] The burden remains on the producing party to make the required showing.[161]

In perhaps the most widely known federal case regarding electronic discovery issues, *Zubulake v. USB Warburg LLC*, the defendant failed to take the necessary steps to ensure that discoverable electronic data was preserved by failing to communicate the litigation hold to all relevant parties.[162] As a result, the production of electronic information was unacceptably delayed and relevant information was destroyed.[163]

Before the Federal Rules were amended, the *Zubulake* court developed a methodical approach (to apply to federal and state litigation) to assess the cost of electronic discovery and to consider if cost shifting is appropriate.[164] In an earlier decision within the *Zubulake* series of cases, the court developed a seven-factor cost-shifting test regarding electronic discovery disputes.[165] Electronic

157. FED. R. CIV. P. 34(b)(ii).

158. FED. R. CIV. P. 34(b)(iii). *But cf.* VA. SUP. CT. R. 4:9(b).

159. *See supra* notes 65–66 and accompanying text.

160. FED. R. CIV. P. 26(b)(2)(B); *cf.* VA. SUP. CT. R. 4:1.

161. FED. R. CIV. P. 26(b)(2)(B).

162. 229 F.R.D. 422, 424 (S.D.N.Y. 2004).

163. *Id.*

164. *Id.*

165. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 322 (S.D.N.Y. 2003). The seven factors were:

> 1. The extent to which the request is specifically tailored to discover relevant information; 2. The availability of such information from other sources; 3. The total cost of production, compared to the amount in controversy; 4. The total cost of production, compared to the resources available to each party; 5. The relative ability of each party to control costs and its incentive to do so; 6.

data can be an amorphous concept, particularly within a business setting where employees generate numerous e-mails, instant messages, and other bits of data as part of their daily activities.[166] Given the vast amounts of electronic data that can be accumulated at both a personal and corporate level, the costs associated with discovery of electronic data in both federal and state litigation can be immense.

The beauty of the new federal system is that even given the unprecedented scale of information stored electronically, the unique impact of electronic data on the discovery process can be managed from the beginning through increased interaction between and disclosure by the parties.[167] Complex issues can be addressed once initial disclosures are made and the parties can rely on the new rules rather than case-by-case decisions on electronic discovery issues.[168] The already robust Virginia common law that has emerged regarding electronic discovery could be greatly enhanced if the Supreme Court of Virginia chose to adopt the amended federal rules.

Lastly, court rules should give clear guidance to the litigants as to what is expected and the consequences of a failure to meet expressed expectations. In the nascent area of the law described in this article, no clearer statement respecting the handling of electronic data in the litigation process is to be found than the following:

> [C]ounsel has a duty to effectively communicate to her client its discovery obligations so that all relevant information is discovered, retained, and produced. In particular, once the duty to preserve attaches, counsel must identify sources of discoverable information . . . . when the duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored. Counsel must also call for employees to produce copies of relevant electronic evidence, and must arrange for the segregation and safeguarding of any archival media . . . that the party has a duty to preserve.

> The importance of the issues at stake in the litigation; and 7. The relative benefits to the parties of obtaining the information.

Id.

166. *See* Krause, *supra* note 155.

167. *See id.*

168. *See id.*

> Once counsel takes these steps (or once a court order is in place), a party is fully on notice of its discovery obligations. If a party acts contrary to counsel's instructions or to a court's order, it acts at its own peril.[169]

VIII. CONCLUSION

Creativity, advocacy, and a respect for precedent have been the guiding lights for the practice of law ever since man came to realize that disputes could be settled in peace. Sometimes these precepts come in conflict. Lawyers and judges will always be challenged to develop new strategies to address novel substantive and procedural issues arising out of the application of the law to emerging technologies. Courts and legislative bodies must continue to determine whether the traditional rules of the adversary process are capable of affording a fair, prompt, and efficient resolution to situations implicating the use of computers, cell phones, pagers, the Internet, iPods, and a host of electronic media.

The Internet has become a personal companion, a home for public debate, a marketplace, a bank, and a library. It offers access to millions of possible readers. Electronic devices have an impact on every aspect of our daily lives—both business and pleasure. What paper was to thousands of years of recorded history, the computer chip is to the future. Virginia has been a leader in the advancement and use of these new technologies and has managed successfully to apply fundamental concepts of law to new technology without compromising judicial values or allowing the new technology to fundamentally change the system. It is the goal of this article to demonstrate to the practitioner that electronic data and other emerging technologies are nothing to be feared.

Electronic data is just that—data. How that data is used is not solely dependent on technology but also on the moral, legal, and ethical standards that benefit from stare decisis and contemporary social thought.

A common law and statutory framework already exists in the Commonwealth to allow for successful litigation strategies that take advantage of the benefits of electronic data. Time-tested le-

---

169. Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 439 (S.D.N.Y. 2004).

gal theories and ethical standards equip practitioners and jurists alike to maintain a principled approach to the practice of law even when technological innovation changes the form of information.

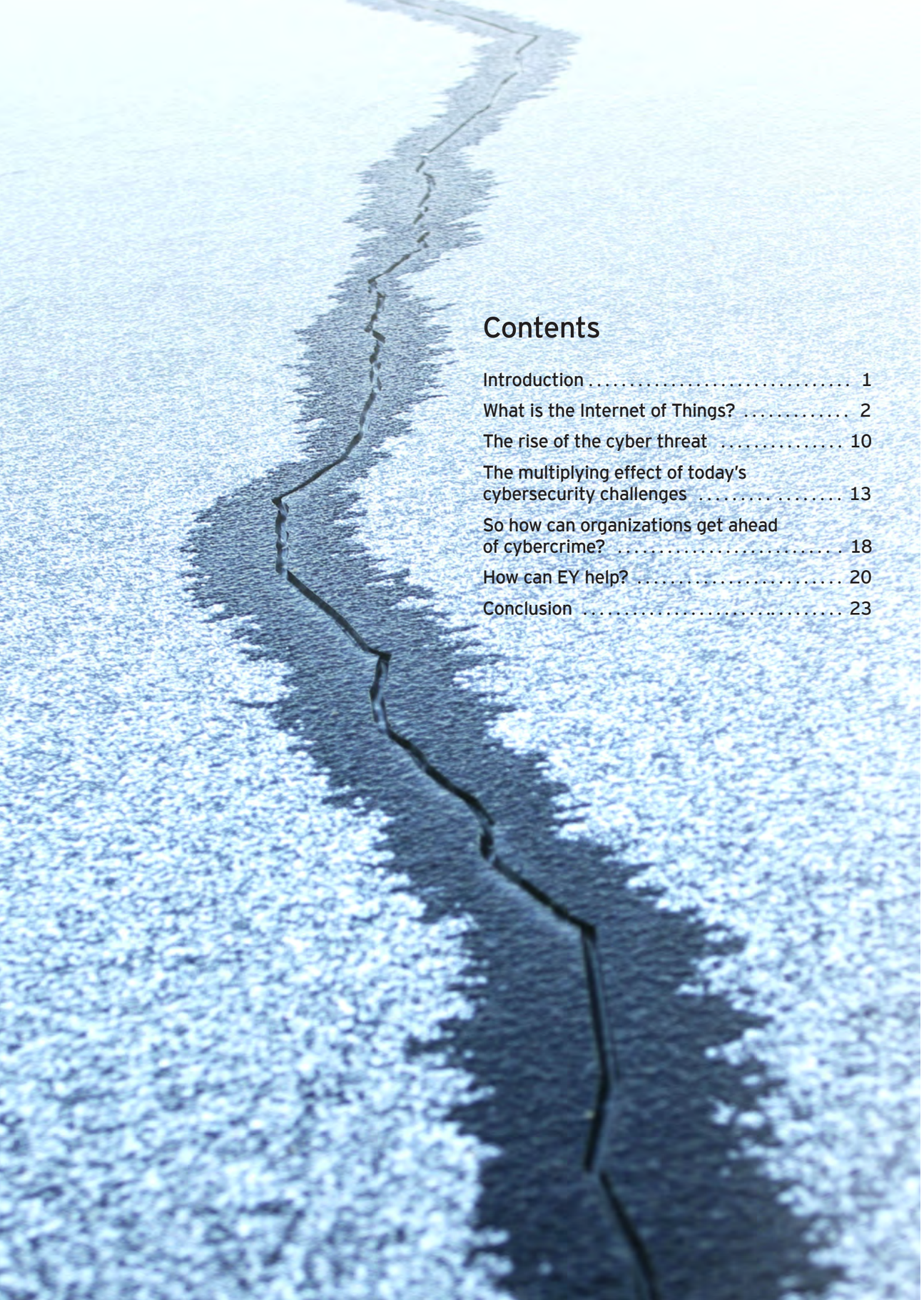
Insights on governance, risk and compliance

March 2015

Cybersecurity and the Internet of Things

EY

Building a better working world



Contents

The growth and spread of connected digital technology

Rapid technological change has resulted in many aspects of our lives being connected and affected by digital communications.

With billions of people connected to the internet today, and the number of connected devices to exceed 50 billion by the year 2020, the Internet of Things (IoT) represents a major transformation in a digital world that has the potential to affect everyone and every business.

IoT can be defined as physical objects that connect to the internet through embedded systems and sensors, interacting with it to generate meaningful results and convenience to the end-user community. The IoT will help to enable an environment with the flexibility to provide services of all sorts, ranging from home automation to smart retail/logistics, and from smart environmental monitoring to smart city services.

In a very short time, the IoT will have sensing, analytics and visualization tools, which can be accessed by anyone, anytime and anywhere in the world on a personal, community or a national level. The potential for it to enable any aspect of our lives is what is encouraging this idea to become established and flourish.

However, the real change is not that machines are talking to each other, but that people are talking more and more "through" machines – the IoT is actually the medium of interconnection for people – and because human communication is mediated by machines and is more and more indirect, there is a deeply rooted security problem with the possibility of impersonation, identity theft, hacking and, in general, cyber threats.

The IoT will increasingly rely on cloud computing, and smart devices with sensors built in, along with thousands (if not millions) of applications to support them. The problem is that the truly integrated environments needed to support this connected technology do not exist, and cloud computing is in need of serious improvement, especially in terms of security.

There is no single object that can be described as the IoT infrastructure – there are many disparate and uneven networks. Because of the increasing stresses on these networks, due to the demands of the data that needs to be supported, many technical areas will need to be redesigned. Additionally, the number of connected devices in circulation being used for the vast amount of interactions has created further challenges in data privacy, data protection, safety, governance and trust.

Taking all of these factors into consideration, we see both opportunities and challenges which require close attention and, in particular, the need for a comprehensive strategic approach to cybersecurity. This report highlights why being in a proactive position to anticipate and mitigate cyber threat is one of today's most important business objectives.

Mobility, digital business models, smart energy infrastructures and the adoption of cutting-edge technologies for transportation, consumer goods and services are transforming cybersecurity concerns. From the back office to the forefront of service quality and business development, security is now embedded in the core strategies of a leading business.

What is the Internet of Things?

The Internet of Things is the network of physical objects that contains embedded technologies to communicate and sense or interact with their internal states or the external environment.

The Internet of Things, Gartner IT. (n.d.). Retrieved from http://www.gartner.com/it-glossary/internet-of-things

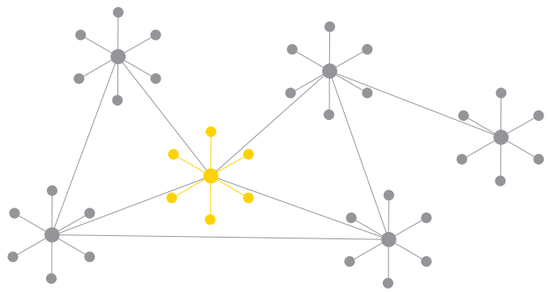
IoT is a future-facing development of the internet wherein objects and systems are embedded with sensors and computing power, with the intention of being able to communicate with each other. Although the original concept of IoT puts excessive emphasis on machine-to-machine communications, the real change underlying this is the diversification of people-to-people communications in an increasingly indirect way. Machines may eventually be able to communicate, but so far this phenomenon is neither universal nor covers all types of networks; even when machines can connect to each other, the fact is that they will remain as instruments of human communications.

The ever-increasing networking capabilities of machines and everyday devices used in the home, office equipment, mobile and wearable technologies, vehicles, entire factories and supply chains, and even urban infrastructure, open up a huge playing field of opportunities for business improvement and customer satisfaction.

Most IoT devices will use sensor-based technologies, in which the sensors will identify or measure any change in position, location, etc.; these sensors will transmit data to a particular device or server, which in turn will analyze the data to generate the "information" for the user. In business terms, the sensors will also act as data gatherers; cloud computing will be a platform for storing and analyzing the data, and Big Data analytics will convert this raw data to knowledge or insights.

Business models for the employment of IoT may vary for every organization, depending upon whether it is handling the core operations, manufacturing or the services/ technologies. The retail and merchandizing sector, for example, could benefit from IoT innovations in the future: if a new customer enters a shoe shop, his or her shoe size could be measured by the measurement sensors; data could be sent over the cloud about availability of stock; the inventory could then be replenished based on real-time analytics and forecasted trends. Other examples for the same retail outlet could be parking sensors, motion sensors, environmental sensors, door sensors that measure footfall, and mobile payment services.

The network of people and things



The network of networks is the full-blown internet of people and things, where every machine-to-machine connection is actually mediated human interaction. These networks are simultaneously networks of collaboration, but also networks of opposition and threat: there is no "inside" or "outside" in this discontinuous, porous space.

IoT is not new

Although IoT is a hot topic today, it's not a new concept. The phrase "Internet of Things" was coined by Kevin Ashton in 1999; the concept was relatively simple, but powerful.

If we had computers that knew everything there was to know about things – using data they gathered without any help from us – we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so.

Kevin Ashton, "That 'Internet of Things' Thing," RFID Journal, July 22, 1999

However, in 1999, there were still more questions than answers to IoT concepts:

- How do we connect everything on the planet?
- What type of wireless communications could be built into devices?
- What changes would be needed to support billions of new devices communicating constantly?
- What would power these devices?
- What must be developed to make the solutions cost-effective?

2015 – enabling technologies driving the successful growth of IoT

- The size and cost of wireless radios has dropped tremendously.
- IPv6 makes it possible to assign a communications address to billions of devices.
- Electronics companies are building Wi-Fi and cellular wireless connectivity into a wide range of devices (e.g., billions of wireless chips).
- Mobile data coverage has improved significantly with many networks offering broadband speeds.
- Battery technology has improved significantly, and solar recharging has been built into numerous devices.

The cloud provides a platform for IoT to flourish, however, there are still many challenges. With the plethora of data that they will hold, storage servers will have to be updated and secured all the time.

Now that we have entered the era of coordination of machine-to-machine, people-to-machine and people-to-people, connections have become much easier.

What opportunities does IoT offer?

IoT is leading change within the digital landscape – and it's fast becoming the must-have element of business technology. Some of the primary forces driving the adoption of IoT are:

- **New business opportunities**
  The web of connected devices, people and data will provide business opportunities to many sectors. Organizations will be able to use IoT data to gain a better understanding of their customers' requirements and can improve processes, such as supply chain/inventory coordination, investments and public safety.
- **Potential for business revenue growth**
  There are multiple untapped opportunities for economic impact by finding creative ways to deploy IoT technology to drive top-line revenue growth and value creation through expense reduction and by improving asset productivity.
- **Improved decision-making**
  Personal computing smart devices are on the rise, leading to wider choice, real-time updates, enhanced facilities, more accurate fact finding, etc. and thus leading to more informed decision-making.
- **Cost reductions**
  The costs of IoT components, such as cloud services, sensors, GPS devices and microchips, have fallen, meaning that the cost of IoT-linked devices is getting more affordable day by day.
- **Safety and security**
  With the help of cameras and sensors, there is the possibility to guard against, or avoid, physical threats, which might occur at the workplace or home. In time, even disaster management or recovery systems will get help from IoT.
- **Improved citizen experience**
  The citizen experience could improve considerably due to ease of access, ease of living and ease of communicating. Think of an example where a citizen can pay his or her taxes remotely, watch his or her parking space from the office, shut down or communicate with gadgets or machines at home, and even proactively monitor his or her health.
- **Improved infrastructure.**
  IoT could help to turn infrastructure into a living organism, especially when major megacities transform into "smart cities." Large population inflow in urban areas and depleted non-renewable energy sources are making resource management a challenge, but intelligent infrastructure and interconnected networks are starting to provide solutions with concepts, such as smart grid, smart waste management, smart traffic control, smart utilities and sustainable city. Microcomputer-enabled automated citizen services will also make future smart cities more secure and more efficient.

The ever-expanding IoT world

IoT is already integrated across several areas where technology adoption is accelerating. The key areas of leading IoT integration are:

Smart life

Innovative, state-of-the-art technology aims to make life simpler and safer for the consumer. Smart life includes:

- **Health care** – a new patient-centric model is emerging
- **Consumer and retail businesses** – the age of the empowered customer and co-creator
- **Banking convergence** – new models for banking and finance
- **Insurance** – moving from statistics to individual fact-based policies
- **Public services** – driving efficiency and convenience for governments and citizens

Smart mobility

Real-time route management and solutions aim to make travel more enjoyable and transportation more reliable. Smart mobility includes:

- **Autonomous driving and the connected car**
- **Urban mobility** – smart traffic management
- **Interurban mobility** – connecting across the transport networks
- **Fare management and payment solutions**
- **Distribution and logistics**
- **Fleet management**

Smart city

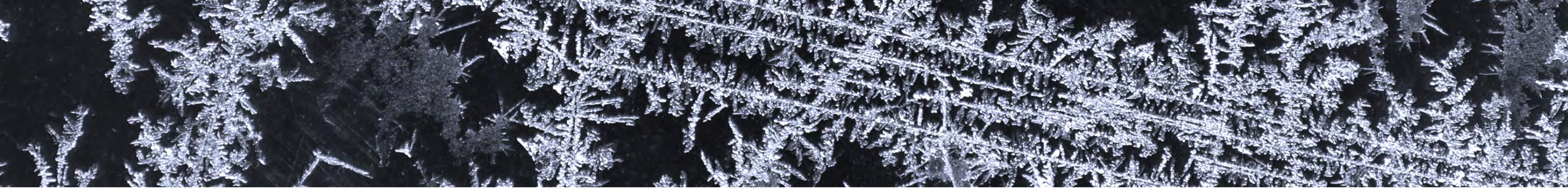
Innovations will aim to improve the quality of life in cities, encompassing security issues and energy resourcefulness. Smart city includes:

- **Smarter management of city infrastructure** – using Big Data analytics
- **Collaboration across multiple and disparate agencies** – using cloud technologies
- **Real-time data collection, enabling quick response** – using mobile technologies
- **Enhanced security** – improved public safety and law enforcement, and more efficient emergency response
- **Better city planning** – improved schematics, project management and delivery
- **Networked utilities** – smart metering and grid management
- **Building developments** – more automation, and better management and security

Smart manufacturing

Factory and logistics solutions will be created specifically to optimize processes, controls and quality. Smart manufacturing includes:

- **Machine learning** – intelligent, automated decision-making
- **Machine communications** - more interaction and collaboration
- **Networking** – networked control and management of manufacturing equipment
- **Optimized processes** – rapid prototyping and manufacturing, improved processes and more efficient supply chain operations
- **Proactive asset management** – via preventive diagnostics and maintenance
- **Better infrastructure integration** – overcoming the interface standards conundrum



Economic benefits of IoT

Just like any other market where demand is directly proportional to the supply, IoT also has a similar economy, with the potential for trillions of dollars of value waiting to be created for both the end users and public and private sector enterprises.

With the growth of IoT, many IT technologies will grow in parallel. For example, cloud computing and Big Data markets give IoT a platform from which to grow and evolve.

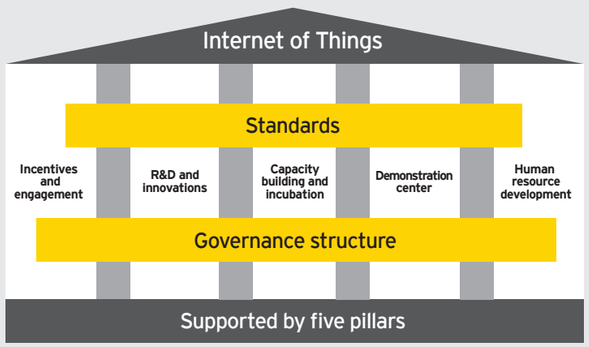
IoT will offer opportunities for companies which are manufacturing IoT goods, and also for those companies which are providing services related to IoT. The manufacturers of smart devices, sensors or actuators, and the application developers, marketing strategists, analytic companies and internet service providers (ISPs) will all profit from the evolution of IoT. According to industry estimates, machine-to-machine (M2M) communications alone will generate approximately US$900 billion in revenues by 2020.

The market is currently focusing on the vertical domains of IoT since it is in relatively early phases of development. But IoT cannot be treated as a single thing, or single platform, or even a single technology. In order to achieve the expected rapid growth from IoT opportunities, more focus needs to be put on interfaces, platforms, mobile applications and common/dominant standards.

IoT policy framework: developing economies' perspective

India is planning to invest approximately US$11 billion for developing 100 smart cities. A draft policy framework document of IoT was released in October 2014 by the Indian government, which proposed the following model.

The two horizontal pillars are standards and governance structure, which are defined as the two governing forces. The future of IoT can be said to be dependent on these two as the former will define the standards for communication, safety, privacy and security, whereas the latter will define the formation, control and power of the government agencies.



Source: Department of Electronics and Information Technology, Government of India

IoT will affect different business sectors in different ways

Key sectors , such as health care, education, financial, retail, communications, hospitality, industry, transportation and agriculture, are already enriched by internet-based technology, and further advancements will make other key economic sectors part of the digital connectivity landscape.

In the past decade, the **health care** sector has been one of the biggest beneficiaries from IoT. Although by no means universal, future solutions may become available such as:

- Personal information that could tell medics not only about individuals' medical history, but also about potential diseases
- Sensors and microcomputers fitted in the human body that could monitor health conditions and even alarm emergency services in case of any distress
  - Similar technology could make living ambience more suitable to an individual's medical requirements
  - Highly automated devices and processes could help to increase critical treatments efficiency with a limited human interface

IoT in the **education** sector has already started to make the conventional education system more automated – interactive smart classrooms are helping students learn and participate more, whilst automatic attendance and various student tracking systems could help to make schools more secure. Internet-enabled remote classrooms will be a milestone for developing countries, making deep penetration in areas where setting up a traditional school infrastructure is not possible.

Internet-enabled **manufacturing and industrial** units are giving differentiating results, making them safer and more efficient through automated process controls. Plant and energy optimization, health and safety control and security management are now increasingly being provided by advanced sensors, networked with sophisticated microcomputers.

Financial services are already leveraging the internet for many of their services. Exponential improvement in digital infrastructure and the next generation of IoT-enabled products could further lead the growth of the financial sector, with innovations, such as smart wearable and smart monitoring devices, helping customers to keep better track of their money and investments.

Telcos could face a surge in data usage due to IoT-enabled devices, thus raising their ARPU (average revenue per user), while on the other hand, they will also have to deal with some concerns, such as privacy and infrastructure security.

> According to industry estimates, machine-to-machine communications alone will generate approximately US$900 billion in revenues by 2020.

The connected car

The connected car is just one way in which IoT is going to impact our lives significantly (and very visibly) in the near future. Here, we address the security requirements of the connected car platform and its environment, but the approach is relevant for all IoT-related innovations.

Connected car security

Similar to the grid (e.g., smart meter) and other mobile and internet-connected systems, the connected car ecosystem should be viewed as a "network of networks" (or a system of systems). The connected car is just one more link (albeit the "newest" one and the most likely to be the focus of attention) in a much wider and complex network.

When taking this point of view, we see the need to shift the emphasis from the connected car as a cleanly defined system, with clear boundaries and input/output points, and take instead as our object of protection the networks themselves, i.e., the interactions between the users/owners of the vehicles and the numerous other actors in the ecosystem. Security becomes then the security of those interactions and is not limited to the car as a "thing."

It is vital to understand the uneven character of digital and network technologies. So, for example, while some studies predict that 70-90% of the motor vehicles may be connected by year 2020, other data indicates that 80% of this connectivity will be very limited (e.g., only through the mobile phone and only for entertainment and "content services"). There won't be universal connections across brands and much less for the entire functionality of the cars for the foreseeable future.

Fundamental change

Because the connected car "lives" in the network, security is not a matter of closing doors and encrypting data; security means managing shared data and a more complex network of participants. Opening the on-board network to the internet means that legacy networks and applications become exposed and the "attack surface" increases as the business model expands to new areas, partners and user types.

The target of protection, the object of security, becomes the network of networks, not the individual car, and all cybersecurity measures and technologies need to be aligned with this goal in mind. Security requirements must be addressed at the application/channel level, but in some cases, this blocks the ability of the auto manufacturer to have a coherent strategy.

When considering connected car initiatives, businesses need to establish a solid legal understanding of data ownership and data protection policies. Only on that basis will it be possible to design agile and secure services that will enhance business operations. So far, in Europe and the rest of the world, issues around data protection do not have a uniform answer yet, and this area requires more work from the angle of information security.

Connected car networks need standard protection measures as security gateways (policy enforcement point) and firewalls (to block DOS and protocol attacks), but this also requires several layers or zones (based on assurance levels and access controls), where each layer implements a security policy. Data ownership and classification must underpin security levels (separate access routes and roles, data path segregation, etc.).

Connecting to multiple trusted and untrusted networks requires a new trust model, but closing the trust gap between the manufacturer and the car owner and between the manufacturer and commercial partners (providers) means balancing risk and trust considerations to create a win-win situation for everyone.

After-sales market and relationship development can be enabled by a security model with clear opt-in and data sharing rules, for example:

- New functions being adopted by the business (e.g., operating incrementally in several roles, including as service providers)
- Business operates in an extended "value chain" with no borders
- New partners are introduced (content providers, etc.)
- Building new relationships with customers (e.g., enabling customers to select products and services online)
- Extending information networks and technologies (e.g., linking transport and distribution networks; or establishing connections with vehicles for service, maintenance and marketing purposes)
- Linking previously physically isolated systems under collaboration networks and enabling remote access (e.g., virtual desktops and software as a service)

The connected car is the focus of EY's *Inside Telecommunications* newsletter, issue 15, 2014: www.ey.com/insidetelco15

The rise of the cyber threat

70%
of the most commonly used IoT devices contain vulnerabilities.

HP study reveals 70% of Internet of Things devices vulnerable to attack. (n.d.). Retrieved from http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc

56%
of respondents say that it is "unlikely or highly unlikely" that their organization would be able to detect a sophisticated attack.**

While the IoT is entering daily life more and more, security risks pertaining to IoT are growing and are changing rapidly. In today's world of "always on" technology and not enough security awareness on the part of users, cyber attacks are no longer a matter of "if" but "when."

Cyber criminals are working on new techniques for getting through the security of established organizations, accessing everything from IP to individual customer information – they are doing this so that they can cause damage, disrupt sensitive data and steal intellectual property.

Every day, their attacks become more sophisticated and harder to defeat. Because of this ongoing development, we cannot tell exactly what kind of threats will emerge next year, in five years' time, or in 10 years' time; we can only say that these threats will be even more dangerous than those of today. We can also be certain that as old sources of this threat fade, new sources will emerge to take their place. Despite this uncertainty – in fact, because of it – we need to be clear about the type of security controls needed.

Effective cybersecurity is increasingly complex to deliver. The traditional organizational perimeter is eroding and existing security defenses are coming under increasing pressure. Point solutions, in particular antivirus software, IDS, IPS, patching and encryption, remain a key control for combatting today's known attacks; however, they become less effective over time as hackers find new ways to circumvent controls.

Cyber attacks have transformed the risk landscape

It's important to remember that cybersecurity is a business-wide issue and not just a technology risk. Since many opportunities for IoT will arise through technological integration and collaboration, which will continue to increase in complexity – this complexity breeds risk.

Traditional proven risk management models have their origins and wisdom still focused in a world where the organization owns and possesses most, if not all, of the data assets flowing through the systems. The increasing use of the internet and mobile working means that the boundary of the enterprise is disappearing: and as a result, the risk landscape also becomes unbounded.

With most of today's business being done outside the organization's defensive fence, it is vital for organizations to be able to communicate with their business partners – and to do this they must create "holes" in the fence. As a result, a cybersecurity system should also include the organization's broader network, including clients, customers, suppliers/vendors, collaborators, business partners and even their alumni – together called the "business ecosystem."

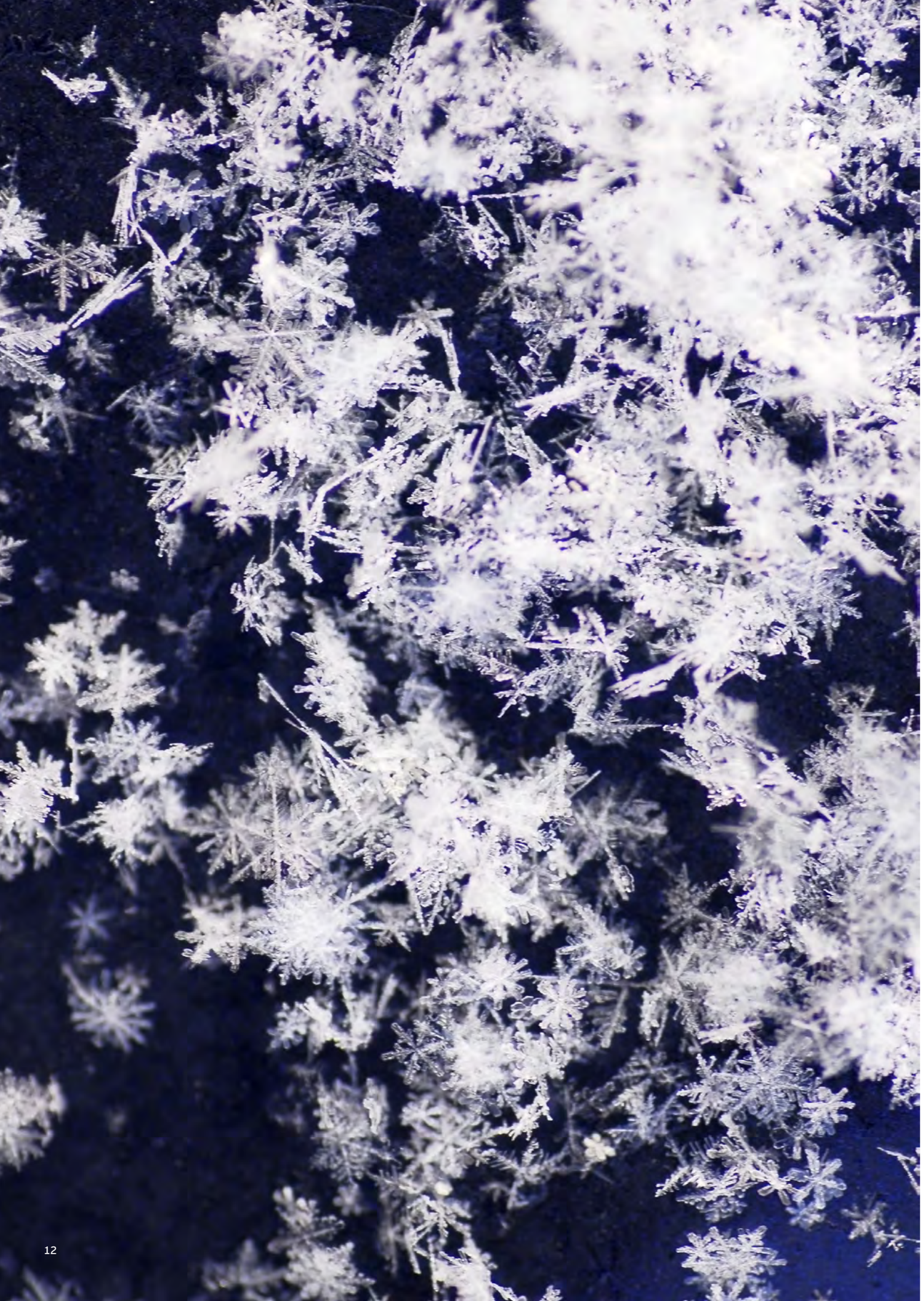
A standard approach to risk management assumes that the trust boundary is already defined. What is missing in the risk-focused and techno-centric approach is everything related to the management of trust, i.e., the new functions and processes, and the new policies and structures required to expand the risk boundary.

An extended ecosystem is governed and managed by various actors with individual policies and assurance requirements; and these actors sometimes have very different interests and business objectives within the collaboration. It is therefore necessary to adjust the organization's normal risk focus to take this into consideration.

For an organization to be able to effectively manage the risks in its ecosystem, it needs to clearly define the limits of that ecosystem. It also needs to decide what it is willing to manage within those boundaries: is it just the risks faced by groups that are one step from the organization itself (e.g., suppliers), or should the organization also try to influence the mitigation of risks faced by groups that are two steps from the center (e.g., the suppliers of suppliers)?

The security of the "thing" is only as secure as the network in which it resides: this includes the people, processes and technologies involved in its development and delivery.

**Survey statistics refer to EY's 17th Global Information Security Survey 2014, which captures the responses of 1,825 C-suite leaders and information security and IT executives/managers, representing most of the world's largest and most-recognized global companies. Responses were received from 60 countries and across nearly all industries. For further information, please access: www.ey.com/GISS2014.



The multiplying effect of today's cybersecurity challenges

The interconnectivity of people, devices and organizations in today's digital world, opens up a whole new playing field of vulnerabilities – access points where the cyber criminals can get in. The overall risk "landscape" of the organization is only a part of a potentially contradictory and opaque universe of actual and potential threats that all too often come from completely unexpected and unforeseen threat actors, which can have an escalating effect.

The speed of change

In this post-economic-crisis world, businesses move fast. New product launches, mergers, acquisitions, market expansion, and introductions of new technology are all on the rise: these changes invariably have a complicating impact on the strength and breadth of an organization's cybersecurity, and its ability to keep pace.

A network of networks

The adoption of mobile computing has resulted in blurring organizational boundaries, with IT getting closer to the user and further from the organization. The use of the internet via smartphones and tablets (in combination with bring-your-own-device strategies by employers) has made an organization's data accessible everywhere and at any time.

Inevitably, one vulnerable device can lead to other vulnerable devices, and it is almost impossible to patch all the vulnerabilities for all the devices. For the cyber criminals, it won't be hard to find a target for their attack. The market of vulnerability (the underground black market selling botnets, zero days, rootkits, etc.) will be vast and so would be the number of victims. It is easier for an attacker to plant a "Trojan" in a phone, if the phone is connected to the computer which has already been compromised. With even more devices connected, it will be even easier for a cyber criminal to get into your attack vector.

Machines or devices will be help people in performing most of their tasks, but consider the scenario when somebody gets a peep into any of our smart devices. In a recent event, the hackers hacked into a baby monitor and after having a good look around at their way in and way out through the camera, they broke into the house.

Infrastructure

Finding loopholes to enter any network will be easier for any attacker since there will be so many ways to attack. Traditionally closed operating technology systems have increasingly been given IP addresses that can be accessed externally, so that cyber threats are making their way out of the back office systems and into critical infrastructures, such as power generation and transportation systems and other automation systems.

Cloud computing

Cloud computing has been a prerequisite for IoT from the very early days of its evolution. The cloud provides a platform for IoT to flourish, however, there are still many challenges which we face today when it comes to cloud security or data security in the cloud. Organizations are often discovering too late that their cloud provider's standards of security may not correspond to their own. The recent events of "CelebGate" and Amazon's IAAS compromise are the live examples of such flaws. These are the incidents which have led the critics to call these services as single point of hack, instead of a single point of storage.

With Big Data also coming into picture, there will be an enormous amount of data produced for the service providers as well. With the plethora of data that they will have, the storage servers will have to be updated and secured all the time. There will be an increase in risks for communication links too, since the sensors and devices will be communicating sensitive personal information all the time on the channels.

With our data stored on such cloud services, there is also a risk of increase in spam as the cloud servers are virtually moved from one geographic location to another in a matter of minutes, depending upon the requirement. Hence, there is no IP-specific blockage possible for any spam.

Application risk

Apps have accelerated the integration of mobile devices within our daily lives. From mapping apps, to social networking, to productivity tools, to games, apps have largely driven the smartphone revolution and have made it as significant and as far-reaching as it is today. While apps demonstrate utility that is seemingly bound only by developer imagination, it also increases the risk of supporting BYOD devices in a corporate environment.

As the organization enables employees to bring their own devices, the need for using the same devices to access work-related data inevitably presents itself. This presents mainly two security risks:

- Malicious apps (malware): the increase in the number of apps on the device increases the likelihood that some may contain malicious code or security holes
- App vulnerabilities: apps developed or deployed by the organization to enable access to corporate data may contain security weaknesses

253 billion

The estimated number of free apps is projected to reach 253 billion by 2017.*

** Retrieved from http://www.statista.com/statistics/241587/number-of-free-mobile-app-downloads-worldwide*

Growing use of mobile devices

Smart phones have already become an integral part of our lives; we rely on them to hold significant information, such as our home address, credit card details, personal photos/videos, e-mail accounts, official documents, contact numbers and messages. The information stored on our devices will include the places that we visit frequently and a "pattern" that uniquely identifies us, so anyone who can hack into any of these devices can get into our lives very easily.

The loss of a single smart device not only means the loss of information, but increasingly it also leads to a loss of identity (identity theft).The internet knows no monopoly and hence all devices cannot have the same firmware or software running on them. Hardware from different companies might not support each other and thus it might lead to interoperability issues of devices.

The increase in the number of devices can also be a problem as the vulnerabilities that they are associated with will spread very rapidly. With thousands of vendors across the globe, it will be very difficult for the network engineers to patch these vulnerabilities, especially with thousands of new patches to update daily – IoT network engineers will now have tenfold devices communicating to their servers outside the network.

Organized cyber criminals will be able to sell hardware with Trojans or backdoors already installed in them, and with the help of these vulnerabilities, they will hunt other victims and make a botnet out of it. These devices, scattered all around the world, will be perfect for a DDOS attack on any of the servers, since sensors don't have antiviruses.

The "bring your own device" employer

With most employees now owning mobile devices, organizations have been exploiting the fact that their employees increasingly want to use their own personal mobile devices to conduct work (often alongside corporate-provided devices), or if an organization requires its employees to do so, it is a cheaper alternative than providing the organization's own. Many organizations are reaching out to corporate IT to support this.

However, BYOD significantly impacts the traditional security model of protecting the perimeter of the IT organization by blurring the definition of that perimeter, both in terms of physical location and in asset ownership. A holistic and methodical approach should be used to define this risk and help to ensure that controls exist to maintain both the security and usability of the devices in the enterprise.

Bandwidth consumption

Thousands of sensors, or actuators, trying to communicate to a single server will create a flood of data traffic which can bring down the server. Additionally, most of the sensors use an unencrypted link to communicate, and hence, there is a possibility of lag in the security.

The bandwidth consumption from billions of devices will put a strain on the spectrum of other wireless communications, which also operate on the megahertz frequencies like radio, television, emergency services, etc. However, companies have started taking this seriously; as a result, Qualcomm has launched its low power Wi-Fi connectivity platform for IoT.

Governance and compliance issues

Increasing privacy legislation is a trend that likely will continue in the near future. As organizations design IoT security controls, these may interfere with personal expectations of privacy. A well-formed IoT policy should include defined, clear expectations on privacy-impacting procedures, bearing in mind that legislation may differ in certain geographical regions.

Privacy and data protection

All smart devices hold information about their users, ranging from their diet plan to where they work; smart devices will include personal life details and often even banking details. All IoT devices gather accurate data from the real world, which is excellent from an analytics prospective, but a user might not be comfortable with sharing that data with a third party – even if not all the data is confidential or sensitive.

With the surfeit of data from billions of devices, there will be plenty of opportunities for analytical organizations; these analytical frameworks will be able to quantify the business environment around the users but, at the same time, the monetization of this data can lead to privacy issues. The question is: do we feel comfortable in sharing our data with people we are not even aware of? Doesn't it feel like a breach into our privacy? Should there be better transparency on how data is stored, used and transported?

According to OWASP (open source web application security project), some of the top privacy risks also contain web application vulnerabilities, operator-side data leakage, insufficient data breach response, data sharing with third parties, and insecure data transfer.

In the application of data protection and privacy law, as well as the access control model, one of the main objectives is that aggregated customer data should not enable anti-competitive, illegal or discriminatory uses. Collection of personal information must be always formally justified (including an impact assessment) and restricted to the minimum necessary for business purposes. According to established regulations, data should be retained for as short a time as possible, strictly to support business operations.

If the organization is collecting personal data, the purpose, expiration, security, etc., of the data collected must be clearly stated in the information security policy. The organization also must undertake a risk assessment of the risks associated with the processing.

If data is processed by a third party (i.e., if the organization utilizes a cloud email provider), it is important that the data be protected by a data processing agreement with the third party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified. However, it is interesting to note that most cloud vendors currently either don't have a privacy policy or have non-transparent policies, which makes users a little uncomfortable about relying on them.

Breach investigation and notification

Following the impact of highly publicized cyber attacks, new and future legislation is proposed on cybersecurity, with fines being levied on companies who do not protect consumer data, and mandatory actions are being introduced around data breach notification. Organizations should prepare for this legislation by keeping an active inventory of devices, the data on them and the security controls in place to protect that data.

Some of the top privacy risks are web application vulnerabilities, operator-side data leakage, insufficient data breach response, data sharing with third parties, and insecure data transfer.*

** OWASP, Top 10 Privacy Risks Project. (n.d.). Retrieved from https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project*

Cybersecurity and smart energy grids

A step change in the evolution of the energy ecosystem

Smart meters and grid infrastructures will generate considerable benefits across the energy lifecycle – from generation through to distribution and consumption. This includes:

- The ability to match supply and demand
- Reduced cost through remote administration of devices
- Better informed consumers through real-time availability of granular energy consumption data

However, if the transition to smart and grid energy management is not developed correctly, there are significant cybersecurity threats to which organizations operating in this space will be exposed.

Smart meter and smart grid complexity

The smart meter infrastructure depends on a wide complex of networked systems, with different technologies and security levels, creating an environment which is difficult to assess from the point of view of data protection and cyber threat management.

Enterprise networks of energy suppliers, each with their own ecosystem, must be connected to the smart meter and grid infrastructure, generating requirements for standardization and regulation of the security mechanisms and processes. The complexity of this environment is not transparent for the general public.

Agreed legitimate uses of stored data need to be complemented with mechanisms to minimize the risk of unauthorized access, including illegal commercialization of data and data retention regulations covering data transferred beyond the original service supplier.

At a technical level, the grid and smart meter infrastructure appears as a network of networks, governed by partnerships and market-driven organizations, with an important input and regulation from the government. These partnerships manage, or will manage, large amounts of consumption and operational data, a fact which calls for a large effort in the direction of a "collaborative security" strategy with specified roles and a joint approach to prevent and repel cyber attacks.

Comprehensive security approach

A multi-faceted, defense-in-depth approach is required to ensure the overall security of the smart metering system. The security solution should aim to protect the system against known and unknown attacks (day zero attacks), unauthorized access, physical tampering, information compromise, denial of service, eavesdropping and other threats.

A set of preventive, detective and corrective controls should be implemented to ensure the security of the smart metering system, which includes end devices, management and monitoring systems, network infrastructure and payment environments. Some of the key controls necessary to meet the smart metering security requirements are: network segregation, data encryption (in transit and rest), near real-time monitoring, device/user authentication solution, device registration/deregistration, etc.

The control environment needs to be supported by a governance framework, appropriate policies and procedures, continuous monitoring and a maturity model to ensure that the overall smart metering system is protected against known and unknown issues and effectively responds to the changing threat landscape.

Customer data privacy and security are critical to ensure customer adoption of smart meters and the expected carbon footprint reduction. The principles of "privacy by design" and "security by design" are required for the implementation of security and privacy, and efforts in this area must be well understood, documented and visible to support the credibility of the solution.

It is important to highlight – as we did in the context of the connected car – that the entire issue of consumer and citizen data protection has not been resolved. There are large differences in legislation between countries and regions, and businesses face the lack of universally accepted technical or industrial standards.

A secure solution could only be achieved by taking a holistic view of the smart metering system and a structured approach to risk management. But to make it truly successful, security must be embedded into the initial solution and not viewed as an "add on."

For further perspectives around smart metering, please see EY's *Plug in* report (November 2014): www.ey.com/smartmeter

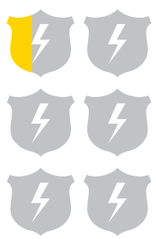
So how can organizations get ahead of cybercrime?

36%

of respondents do not have a threat intelligence program.**

37%

say that real time insight on cyber risk is not available.**



6%

of organizations claim to have a robust incident response program that includes third parties and law enforcement and is integrated with their broader threat and vulnerability management function.**

Your organization may already have strong IT policies, processes and technologies, but, is it prepared for what is coming? Early warning and detection of breaches are decisive to being in a state of readiness, meaning that the emphasis of cybersecurity has changed to threat intelligence. Most organizations already know that there are threats for their information and operational systems, as well as for their products – the step beyond is to understand the nature of those threats and how these manifest themselves.

An organization in a state of readiness to deal with cyber attacks inhabits an entirely different mind-set, sees the world differently and responds in a way the cyber criminals would not expect. It requires behaviors that are thoughtful, considered and collaborative. It learns, prepares and rehearses. No organization or government can ever predict or prevent all (or even most) attacks; but they can reduce their attractiveness as a target, increase their resilience and limit damage from any given attack.

A state of readiness includes:

- Designing and implementing a cyber threat intelligence strategy to support strategic business decisions and leverage the value of security
- Defining and encompassing the organizations extended cybersecurity ecosystem, including partners, suppliers, services and business networks
- Taking a cyber economic approach – understanding your vital assets and their value, and investing specifically in their protection
- Using forensic data analytics and cyber threat intelligence to analyze and anticipate where the likely threats are coming from and when, increasing your readiness
- Ensuring that everyone in the organization understands the need for strong governance, user controls and accountability

Organizations may not be able to control when information security incidents occur, but they can control how they respond to them – expanding detection capabilities is a good place to start. A well-functioning security operations center (SOC) can form the heart of effective detection.

Managing cyber threats according to business priorities must be the focus of the SOC. By correlating business-relevant information against a secure baseline, the SOC can produce relevant reporting, enabling better decision-making, risk management and business continuity. An SOC can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.

Follow leading cybersecurity practices

By leveraging-industry leading practices and adopting strategies that are flexible and scalable, organizations will be better equipped to deal with incoming (sometimes unforeseen) challenges to their security infrastructure.

As technology advances and companies continue to innovate over the coming years, organizations using the IoT will need to continuously assess the security implications of adopting these advancements. A consistent and agile multi-perspective security risk assessment methodology will help to evaluate the organizations risk exposure. The introduction of appropriate procedures and regular testing will help organizations become smarter and make their employees more aware of the challenges that IoT poses for the entire enterprise.

- **Know your environment, inside and out**
  Comprehensive, yet targeted, situational awareness is critical to understanding the wider threat landscape and how it relates to the organization. Cyber threat intelligence can bring this knowledge – it incorporates both external and internal sources of risk, and covers both the present and future, while learning from the past.
- **Continually learn and evolve**
  Nothing is static – not the criminals, not the organization or any part of its operating environment – therefore the cycle of continual improvement remains. Become a learning organization: study data (including forensics), maintain and explore new collaborative relationships, refresh the strategy regularly and evolve cybersecurity capabilities.
- **Be confident in your incident response and crisis response mechanisms**
  Organizations that are in a state of anticipation regularly rehearse their incident response capabilities. This includes war gaming and table top exercises, through to enacting complex incident scenarios that really test the organization's capabilities.
- **Align cybersecurity to business objectives**
  Cybersecurity should become a standing boardroom issue – a vitally important item on the agenda. The organization's leadership should understand and discuss how cybersecurity enables the business to innovate, open new channels to market and manage risk. To be successful, the information security function needs leadership support in providing the appropriate revenue to support and grow better security protection, to promote cybersecurity awareness within the workforce, and to sponsor cooperation with business peers.

Move from security as a cost, to security as a plus

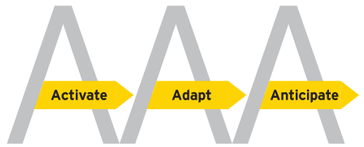
Security is usually positioned as an obligatory cost – a cost to pay to be compliant, or a cost to pay to reduce risk. But moving to a model of security as risk and trust management implies looking upon security as a business enabler; for example, managing consumer data access leverages the monetary value of the data instead of focusing on the protection of the data itself. In fact, this transformation means enabling the development of even more extended networks of networks, of more and new forms of collaboration and mobility, and of new business models. **"Security as a plus" should be a mainstay of the business.**

The future of IoT

"Dubbed by many as nothing less than the "3rd industrial revolution", the Internet of Things is one of the digital game changers. We believe that when everyone and everything is connected within seamless information networks and the resulting data is evaluated by intelligent and predictive big data analytics, and with robust cybersecurity measures in place, we will see positive changes in the way we all conduct business; how we operate our factories, supply chains and logistics networks; how we manage our infrastructure; and last but not least, how we as consumers, patients and citizens interact with suppliers, retailers, health care providers and government agencies."

Paul van Kessel, EY Global Risk leader

How can EY help?



EY has identified that organizations' responses to cybercrime fall into three distinct stages of cybersecurity maturity – Activate, Adapt and Anticipate (the three As) – and the aim should be to implement ever more advanced cybersecurity measures at each stage.

Stage 1: Activate

Organizations need to have a solid foundation of cybersecurity. This comprises a comprehensive set of information security measures, which will provide basic (but not good) defense against cyber attacks. At this stage, organizations establish their fundamentals – i.e., they "activate" their cybersecurity.

Stage 2: Adapt

Organizations change – whether for survival or for growth. Threats also change. Therefore, the foundation of information security measures must adapt to keep pace and match the changing business requirements and dynamics otherwise they will become less and less effective over time. At this stage, organizations work to keep their cybersecurity up-to-date; i.e., they "adapt" to changing requirements.

Stage 3: Anticipate

Organizations need to develop tactics to detect and detract potential cyber attacks. They must know exactly what they need to protect their most valuable assets, and rehearse appropriate responses to likely attack/incident scenarios: this requires a mature cyber threat intelligence capability, a robust risk assessment methodology, an experienced incident response mechanism and an informed organization. At this stage, organizations are more confident about their ability to handle more predictable threats and unexpected attacks; i.e., they anticipate cyber attacks.

What it is	Cybersecurity system building blocks	Status
Anticipate is about looking into the unknown. Based on cyber threat intelligence, potential hacks are identified; measures are taken before any damage is done.	**Anticipate**	**Anticipate** is an emerging level. More and more organizations are using cyber threat intelligence to get ahead of cybercrime. It is an innovative addition to the below.
Adapt is about change. The cybersecurity system is changing when the environment is changing. It is focused on protecting the business of tomorrow.	**Adapt**	**Adapt** is not broadly implemented yet. It is not common practice to assess the cybersecurity implications every time an organization makes changes in the business.
Activate sets the stage. It is a complex set of cybersecurity measures focused on protecting the business as it is today.	**Activate**	**Activate** is part of the cybersecurity system of every organization. Not all necessary measures are taken yet; there is still a lot to do.

Helping you anticipate cybercrime

We have seen that organizations need to change their way of thinking to stop being simply reactive to future threats; yet in our recent Global Information Security Survey (www.ey.com/cybersecurity) we found that only 5% of the 1,800 organizations surveyed had a threat intelligence team with dedicated staff.

The only way to get ahead of the cyber criminals is to learn how to anticipate their attacks; this means that your cybersecurity capability should be able to address the following questions:

- What is happening out there that our organization needs to learn from?
- How are other successful organizations dealing with threats and attacks?
- How can our organization become "hardened" against attack?
- Can our organization distinguish a random attack from a targeted one?
- What would be the economic cost of an attack?
- How would our customers be impacted by an attack?
- What would the legal and regulatory consequences of a serious attack be?
- How can we help others in our ecosystem deal with threats and attacks?

EY can help organizations improve their ability to respond to changes in the threat landscape. We provide services to assist organizations in developing in-house threat intelligence programs as well as several key threat intelligence services in subscription-based models and full spectrum managed cyber threat intelligence services.

We believe that security assessments are an effective method of identifying vulnerabilities and understanding their impact. Together with IT security, risk management and internal audit groups at our clients, we contextualize these technical findings within the business to fully understand the risk to the most critical assets. It is this teaming between technical testers and business owners that we believe will continue to be the most effective method of evaluating the security of both established and emerging technologies.

Using EY's security practices and industry leading experience, we help our clients secure both the device ecosystem and assess security at the network level, and we assist our clients in defining and implementing state-of-the-art security controls to:

- Secure the data from device to data center to the cloud
- Manage large volumes of data, utilizing our knowledge of data analytics
- Comply with the applicable security and regulatory requirements
- Standardize the security controls for their offerings, thereby creating faster go-to-market capabilities

However, we appreciate that many of our clients face location, time and cost constraints, which make it difficult to determine what security measures are cost-effective and make sense within the business strategy. We can help our clients gain a thorough understanding of the options.

58%

of organizations do not have a role or department focused on emerging technologies and their impact on information security.**

IoT must change the way businesses do business

There is no doubt that IoT is changing the way we all live and work. There are many opportunities for the public as well as private sector markets through technological integration and collaboration.

New innovations are being introduced daily, but along with these, threats are being created which will challenge your organization. You need to get ahead of the game now to be successful tomorrow.

IoT will increasingly have sensing, analytics and visualization tools that may be accessed on a personal, community or national level. Information sharing and ease of accessibility via the IoT makes businesses vulnerable to targeted cyber attacks, so the huge benefits must be weighed against the growing risks.

> IoT offers tremendous opportunities for personal improvements and for business innovation, but innovators need to be aware of the risks involved in IoT to provide better and more powerful solutions for the world.
>
> *Ken Allan, Global Cybersecurity Leader, EY.*

As a consequence of IoT adoption, together with supporting technologies and services based on cloud infrastructure and mobile devices, enterprise security requirements have to be addressed with a focus on the relationships between the organization and its environment.

Organizations must adapt and look ahead and beyond the current business. With the understanding that attacks can never be fully prevented, companies should advance their cyber threat detection capabilities so they can respond appropriately and proactively.

Learning how to stay ahead of cybercrime is challenging and takes time, but the benefits for the organization are considerable – the organization will be able to exploit the opportunities offered by the digital world, while minimizing exposure to risks and the cost of dealing with them.

Next steps

Take a look at your organization (public, private or NGO). What can you do that you couldn't do before? Start to do it now, before someone else does. "Act" rather than "react."

Consider these key questions:

- What IoT capabilities does your organization have today?
- Can you harness the complementary insights of both service and IT leaders?
- Have you identified major IoT opportunity areas that link with your vision and strategy?
- Can you build an "IoT culture" around the possibilities of connecting the unconnected?
- How will IoT change the basis of competition?
- How will you delight customers as everything gets connected?
- Do your business plans reflect the full potential of IoT?
- Are your technology investments aligned with opportunities and threats?
- How will IoT improve your agility?
- Do you have the capabilities to deliver value from IoT?
- What is your accountability and governance structure/ model for IoT execution?
- How are the risks associated with IoT being addressed?
- How will you communicate about IoT to stakeholders?

If you are unsure about any of these answers, speak to your EY representative.

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please visit our *Insights on governance, risk and compliance* series at www.ey.com/GRCinsights.

Get ahead of cybercrime: *EY's Global Information Security Survey 2014*

www.ey.com/GISS

Achieving resilience in the cyber ecosystem

www.ey.com/cyberecosystem

Bring your own device: *security and risk considerations for your mobile device program*

www.ey.com/byod

Security Operations Centers – helping you get ahead of cybercrime

www.ey.com/SOC

Cyber Program Management: *identifying ways to get ahead of cybercrime*

www.ey.com/CPM

Cyber threat intelligence – how to get ahead of cybercrime

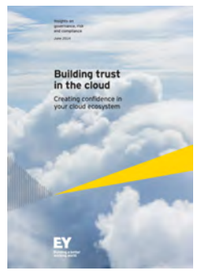
www.ey.com/CTI

Maximizing the value of a data protection program

www.ey.com/dataprotect

Big data: *changing the way businesses compete and operate*

www.ey.com/bigdatachange



Building trust in the cloud: *creating confidence in your cloud ecosystem*

www.ey.com/cloudtrust

At EY, we have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance as well as enterprise risk management.

We innovate in areas, such as risk consulting, risk analytics and risk technologies, to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our client's applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. AU2979
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/GRCinsights

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or, more specifically, on achieving growth or optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/advisory

Our Risk Advisory leaders are:

Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp

Our Cybersecurity leaders are:

Global Cybersecurity Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Area Cybersecurity Leaders		
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
EMEIA		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Asia-Pacific		
Paul O'Rourke	+65 6309 8890	paul.orourke@sg.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp

The White House
Office of the Press Secretary

For Immediate Release May 11, 2017

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

EXECUTIVE ORDER

- - - - - - -

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings.

(i) Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

(ii) The executive branch has for too long accepted antiquated and difficult–to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance.

(v) Effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources.

(c) Risk Management.

(i) Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.

(ii) Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order. The risk management report shall:

(A) document the risk mitigation and acceptance choices made by each agency head as of the date of this order, including:

(1) the strategic, operational, and budgetary considerations that informed those choices; and

(2) any accepted risk, including from unmitigated vulnerabilities; and

(B) describe the agency's action plan to implement the Framework.

(iii) The Secretary of Homeland Security and the Director of OMB, consistent with chapter 35, subchapter II of title 44, United States Code, shall jointly assess each agency's risk management report to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate (the determination).

(iv) The Director of OMB, in coordination with the Secretary of Homeland Security, with appropriate support from the Secretary of Commerce and the Administrator of General Services, and within 60 days of receipt of the agency risk management reports outlined in subsection (c)(ii) of this section, shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the following:

(A) the determination; and

(B) a plan to:

(1) adequately protect the executive branch enterprise, should the determination identify insufficiencies;

(2) address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(3) establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(4) clarify, reconcile, and reissue, as necessary and to the extent permitted by law, all policies, standards, and guidelines issued by any agency in furtherance of chapter 35, subchapter II of title 44, United States Code, and, as necessary and to the extent permitted by law, issue policies, standards, and guidelines in furtherance of this order; and

(5) align these policies, standards, and guidelines with the Framework.

(v) The agency risk management reports described in subsection (c)(ii) of this section and the determination and plan described in subsections (c)(iii) and (iv) of this section may be classified in full or in part, as appropriate.

(vi) Effective immediately, it is the policy of the executive branch to build and maintain a modern, secure, and more resilient executive branch IT architecture.

(A) Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.

(B) The Director of the American Technology Council shall coordinate a report to the President from the Secretary of Homeland Security, the Director of OMB, and the Administrator of General Services, in consultation with the Secretary of Commerce, as appropriate, regarding modernization of Federal IT. The report shall:

(1) be completed within 90 days of the date of this order; and

(2) describe the legal, policy, and budgetary considerations relevant to -- as well as the technical feasibility and cost effectiveness, including timelines and milestones, of -- transitioning all agencies, or a subset of agencies, to:

(aa) one or more consolidated network architectures; and

(bb) shared IT services, including email, cloud, and cybersecurity services.

(C) The report described in subsection (c)(vi)(B) of this section shall assess the effects of transitioning all agencies, or a subset of agencies, to shared IT services with respect to cybersecurity, including by making recommendations to ensure consistency with section 227 of the Homeland Security Act (6 U.S.C. 148) and compliance with policies and practices issued in accordance with section 3553 of title 44, United States Code. All agency heads shall supply such information concerning their current IT architectures and plans as is necessary to complete this report on time.

(vii) For any National Security System, as defined in section 3552(b)(6) of title 44, United States Code, the Secretary of Defense and the Director of National Intelligence, rather than the Secretary of Homeland Security and the Director of OMB, shall implement this order to the maximum extent feasible and appropriate. The Secretary of Defense and the Director of National Intelligence shall provide a report to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism describing their implementation of subsection (c) of this section within 150 days of the date of this order. The report described in this subsection shall include a justification for any deviation from the requirements of subsection (c), and may be classified in full or in part, as appropriate.

Sec. 2. Cybersecurity of Critical Infrastructure.

(a) Policy. It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure (as defined in section 5195c(e) of title 42, United States Code) (critical infrastructure entities), as appropriate.

(b) Support to Critical Infrastructure at Greatest Risk. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and

Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall:

(i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

(ii) engage section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities identified pursuant to subsection (b)(i) of this section might be employed to support cybersecurity risk management efforts and any obstacles to doing so;

(iii) provide a report to the President, which may be classified in full or in part, as appropriate, through the Assistant to the President for Homeland Security and Counterterrorism, within 180 days of the date of this order, that includes the following:

(A) the authorities and capabilities identified pursuant to subsection (b)(i) of this section;

(B) the results of the engagement and determination required pursuant to subsection (b)(ii) of this section; and

(C) findings and recommendations for better supporting the cybersecurity risk management efforts of section 9 entities; and

(iv) provide an updated report to the President on an annual basis thereafter.

(c) Supporting Transparency in the Marketplace. The Secretary of Homeland Security, in coordination with the Secretary of Commerce, shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, that examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities, within 90 days of the date of this order.

(d) Resilience Against Botnets and Other Automated, Distributed Threats. The Secretary of Commerce and the Secretary of Homeland Security shall jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets). The Secretary of Commerce and the Secretary of Homeland Security shall consult with the Secretary of Defense, the Attorney General, the Director of the Federal Bureau of Investigation, the heads of sector-specific agencies, the Chairs of the Federal Communications Commission and Federal Trade Commission, other interested agency heads, and appropriate stakeholders in carrying out this subsection. Within 240 days of the date of this order, the Secretary of Commerce and the Secretary of Homeland Security shall make publicly available a preliminary report on this effort. Within 1 year of the date of this order, the Secretaries shall submit a final version of this report to the President.

(e) Assessment of Electricity Disruption Incident Response Capabilities. The Secretary of Energy and the Secretary of Homeland Security, in consultation with the Director of National Intelligence, with State, local, tribal, and territorial governments, and with others as appropriate, shall jointly assess:

(i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident, as defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination), against the United States electric subsector;

(ii) the readiness of the United States to manage the consequences of such an incident; and

(iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

(f) Department of Defense Warfighting Capabilities and Industrial Base. Within 90 days of the date of this order, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, in coordination with the Director of National Intelligence, shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks. The report may be classified in full or in part, as appropriate.

Sec. 3. Cybersecurity for the Nation.

(a) Policy. To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.

(b) Deterrence and Protection. Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the United States Trade Representative, in coordination with the Director of National Intelligence, shall jointly submit a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats.

(c) International Cooperation. As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining the policy set forth in this section. Within 45 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Commerce, and the Secretary of Homeland Security, in coordination with the Attorney General and the Director of the

Federal Bureau of Investigation, shall submit reports to the President on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. Within 90 days of the submission of the reports, and in coordination with the agency heads listed in this subsection, and any other agency heads as appropriate, the Secretary of State shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, documenting an engagement strategy for international cooperation in cybersecurity.

(d) Workforce Development. In order to ensure that the United States maintains a long-term cybersecurity advantage:

(i) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, shall:

(A) jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and

(B) within 120 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

(ii) The Director of National Intelligence, in consultation with the heads of other agencies identified by the Director of National Intelligence, shall:

(A) review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness; and

(B) within 60 days of the date of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism on the findings of the review carried out pursuant to subsection (d)(ii)(A) of this section.

(iii) The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence, shall:

(A) assess the scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and

(B) within 150 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations on the assessment carried out pursuant to subsection (d)(iii)(A) of this section.

(iv) The reports described in this subsection may be classified in full or in part, as appropriate.

Sec. 4. Definitions. For the purposes of this order:

(a) The term "appropriate stakeholders" means any non-executive-branch person or entity that elects to participate in an open and transparent process established by the Secretary of Commerce and the Secretary of Homeland Security under section 2(d) of this order.

(b) The term "information technology" (IT) has the meaning given to that term in section 11101(6) of title 40, United States Code, and further includes hardware and software systems of agencies that monitor and control physical equipment and processes.

(c) The term "IT architecture" refers to the integration and implementation of IT within an agency.

(d) The term "network architecture" refers to the elements of IT architecture that enable or facilitate communications between two or more IT assets.

Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be construed to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence or law enforcement operations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

THE WHITE HOUSE,
May 11, 2017.

User Name: Kyle Armstrong

Date and Time: Tuesday, October 17, 2017 5:25:00 PM EDT

Job Number: 55130569

Document (1)

1. *SYMPOSIUM: Cyberwars: Navigating Responsibilities for the Public and Private Sector: Legal Ethics' Next Frontier: Lawyers and Cybersecurity, 19 Chap. L. Rev. 501*

   Client/Matter: -None-

   Search Terms: SYMPOSIUM: Cyberwars: Navigating Responsibilities for the Public and Private Sector: Legal Ethics' Next Frontier: Lawyers and Cybersecurity, 19 Chap. L. Rev. 501

   Search Type: Natural Language

SYMPOSIUM: Cyberwars: Navigating Responsibilities for the Public and Private Sector: Legal Ethics' Next Frontier: Lawyers and Cybersecurity

Spring, 2016

Reporter
19 Chap. L. Rev. 501 *

Length: 21273 words

Author: Eli Wald*

* Charles W. Delaney Jr. Professor of Law, University of Denver Sturm College of Law. I thank Denis Binder, Tanya Forsheit, Scott Garner, Marty Katz, Ron Rotunda, Drew Simshaw, and other participants in the "Cyber Wars: Navigating Responsibilities for the Public and Private Sector" Symposium at Chapman University Dale E. Fowler School of Law for their helpful comments. I also thank Diane Burkhardt, Faculty Services Liaison at the Westminster Law Library at the University of Denver Sturm College of Law, for her outstanding research assistance.

Text

[*501]

The publication of the Panama Papers containing confidential client information, following a cybersecurity breach at the law firm of Mossack Fonseca, demonstrated what many have long known, that law firms are particularly vulnerable to cyberattacks. [1] Yet since concerns about law firms' cyber practices have first surfaced, the legal profession has learned a lot about cybersecurity. We know who is perpetrating cyberattacks against lawyers, we know why they are doing it, and we even know quite a bit about how to prevent and defend against attacks, as well as how to mitigate their damage and respond when an attack takes place. Still, there are quite a few things we do not know. Most importantly, we do not know the extent and scope of cyberattacks against law firms, and we do not know whether lawyers are acting on the growing body of cybersecurity knowledge they possess to reasonably protect their clients' information from unauthorized access. Indeed, we have reason to believe that some **[*502]** lawyers, notwithstanding their awareness of cybersecurity threats, fail to take reasonable steps to protect themselves and their clients, because they are underregulated, likely to escape any meaningful consequences for their inaction, and therefore, have little incentive to take reasonable cybersecurity action.

Lawyers' cybersecurity conduct is underregulated because the usual regulatory suspects, liability rules and market controls, do not rigorously apply. Since proving cybersecurity damages is often hard to do, lawyers do not systematically face the prospect of malpractice liability for failing to adequately protect clients' information. Since lawyers are generally under no duty to report cyberattacks to their clients or to others, they do not face market

---

[1] On the Panama Papers, see Luke Harding, What Are the Panama Papers? A Guide to History's Biggest Data Leak, Guardian (Apr. 5, 2016), http://www.theguardian.com/ news/2016/apr/03/what-you-need-to-know-about-the-panama-papers [http://perma.cc/PG79-Z7HM]; David Z. Morris, The Laughably Bad Security at "Panama Papers' firm Mossack Fonseca, Fortune (Apr. 9, 2016), http://fortune.com/2016/04/09/bad-security-panama-papers/ [http://perma.cc/453A-ZXZB]. The Federal Bureau of Investigation publicly identified law firms as vulnerable in 2009, see Susan Hansen, Cyber Attacks Upend Attorney-Client Privilege, Bloomberg (Mar. 19, 2015, 11:56 AM), http://www.bloomberg.com/news/ articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security [http://perma.cc/ 8LSR-5UEQ]. The FBI reiterated its caution in 2011, calling on major law firms to raise their level of awareness regarding cyberattacks. See Anne Marie Davine, More Cyber Preparedness Needed, According to 2014 Law Firm Cyber Survey, Marsh (Jan. 15, 2015), https://www.marsh. com/us/insights/more-cyber-preparedness-needed-2014-law-firm-cyber-survey.html [http://perma.cc/5SFK-TTQ9]. FBI officials and security experts maintain that law firms remain a weak link when it comes to online security. Id.

sanctions, such as being fired or suffering reputational losses. Of course, some lawyers have been at the forefront of practicing diligent cybersecurity. Yet, because practicing cybersecurity is expensive and the technological learning curve for lawyers is steep, in the face of underregulation and few practical consequences for inaction, some lawyers may fail to reasonably defend against cyberthreats, the known risks notwithstanding. [2] Moreover, because malpractice lawsuits are scarce, there is little in the way of judicial exposition of the meaning of reasonable cybersecurity practices, leaving even those lawyers who are committed to practicing reasonable cybersecurity in the dark.

This Article argues that the underregulation of lawyers' cybersecurity conduct may be addressed by the promulgation of robust rules of professional conduct, delineating the meaning of reasonable cybersecurity protections and mandating greater disclosure of unauthorized access to clients. Effective rules of professional conduct are likely to incentivize lawyers to take action for three related reasons. First, the threat of discipline will motivate some lawyers to take reasonable cybersecurity action and advise clients when attacks result in compromised information. Second, a mandatory disclosure duty will in turn enable more effective market regulation as clients will be able to sanction lawyers for inaction. Third, the promulgation of effective cybersecurity rules may result in peer pressure and the development of reasonable cybersecurity social norms among lawyers.

Part I of the Article summarizes the knowledge lawyers have recently gained about cybersecurity, namely, who is attacking them, why, and what can be done to defend against cyberattacks. **[*503]** Part II examines the underregulation of lawyers' cybersecurity conduct and its consequences. Part III advances a proposal for a regulatory response, in the form of new and revised rules of professional conduct.

I. The State of Lawyers' Cybersecurity Knowledge

The use of technology is pervasive in the practice of law. Like many other professions, lawyers e-mail, store information remotely, share files, and use mobile devices and wireless networks; their "widespread use of electronic records and mobile devices" presents "unprecedented challenges." [3] As The ABA Cybersecurity Handbook explains, "creating, using, communicating, and storing information in electronic form greatly increases the potential for unauthorized access, use, disclosure, and alteration, as well as the risk of loss or destruction." [4] Lawyers must understand and respond to these risks in order to protect confidential client information, which if compromised, can expose clients to the loss of the attorney-client privilege, fraud, negative publicity and tarnished business reputations, liability to others, and even bankruptcy. [5]

Over the last few years, however, the legal profession has learned a great deal about cybersecurity. Lawyers now know why they have become likely targets for hackers, who is perpetrating the attacks, and what they can do to minimize the probability and severity of attacks before they take place, as well as respond to attacks when they happen. This part briefly summarizes the growing wealth of information about cybersecurity.

A. Why Lawyers Are Under (Cyber) Attack

---

[2] James R. Silkenat, Privacy and Data Security for Lawyers, *38 Am. J. Trial Advoc. 449, 454 (2015)* ("But in the case of cybersecurity, attorneys sometimes take a more "do as I say, not as I do' approach.").

[3] ABA Cybersecurity Legal Task Force & Section of Science & Technology Law, Report to the House of Delegates: Resolution 109, ABA 4 (Aug. 2014) [hereinafter ABA Cybersecurity Resolution], *http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions /2014_hod_annual_meeting_109.authcheckdam.pdf* [*http://perma.cc/NS7C-JXS7*].

[4] Jill D. Rhodes & Vincent I. Polley, The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals 41 (2013). See generally Marc Goodman, Future Crimes - Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About IT (2015).

[5] Drew T. Simshaw, Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data, *38 Am. J. Trial Advoc. 549, 550, 554 (2015).*

Lawyers experience cyberattacks for three related reasons: they store valuable confidential client information, they are likely to be more vulnerable than their clients, and they are under increased pressure to take advantage of technologies that render them susceptible to attacks. To begin with, cybersecurity is traditionally concerned with protecting confidential information, **[*504]** maintaining the integrity of information, and ensuring the availability of stored information. [6] Protecting confidential information is especially important to the legal profession, as all lawyers and law firms are depositories of valuable confidential information related to the representation of clients. As the American Bar Association Model Rules of Professional Conduct ("Rules") explain, protecting confidential information is a "fundamental principle" that "contributes to the trust that is the hallmark of the client-lawyer relationship." [7] Confidentiality encourages clients "to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively." [8] Put differently, to effectively represent clients, lawyers routinely collect and store valuable client information. Because lawyers receive and store valuable confidential information pertaining to their clients' matters, they are likely targets for hackers.

Context always matters in the practice of law, [9] and it is essential to gaining an understanding of the cybersecurity practices of lawyers. Different types of law firms offer different types of potential value to hackers in terms of the confidential client information they store. For example, hacking large law firms, which tend to represent large entity clients, [10] is often more **[*505]** efficient than hacking each of the law firms' large entity clients individually. [11] Large entity clients tend to store enormous quantities of information, though much of it may be of relatively little value to hackers, even if they had the resources to comb through it following a successful attack. For hackers, large law firms are a one-stop shop, [12] serving as filters of low value material, [13] because BigLaw will tend to receive from its clients and store only a subset of their vast information, namely, the valuable portion of it. Thus, while one

---

[6] David G. Delaney, Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation, *40 J. Legis. 251, 251 (2014)* ("At its core, cybersecurity involves information security or assurance - preserving the confidentiality, availability, and integrity of information."). The core objectives of confidentiality, availability, and integrity of information inform cybersecurity legislation. For example, under the Health Insurance Portability and Accountability Act, covered entities "must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected." See Health Insurance Reform: Security Standards, *68 Fed. Reg. 8334, 8334* (Feb. 20, 2003). Similarly, the National Institute of Standards and Technology ("NIST"), a Department of Commerce non-regulatory agency, "provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services." See Computer Security Resource Center, NIST, *http://www.nist.gov/itl/csd/csrc.cfm* [*http://perma.cc/K7RV-XMPR*] (last updated Oct. 5, 2010).

[7] Model Rules of Prof'l Conduct r. 1.6 cmt. 2 (Am. Bar Ass'n 2013).

[8] Id.

[9] Eli Wald, Resizing the Rules of Professional Conduct, *27 Geo. J. Legal Ethics 227, 235-44 (2014);* David B. Wilkins, Legal Realism for Lawyers, *104 Harv. L. Rev. 468, 473, 476, 515-19 (1990);* David B. Wilkins, Who Should Regulate Lawyers?, *105 Harv. L. Rev. 799, 814-19 (1992).* See generally David B. Wilkins, Making Context Count: Regulating Lawyers After Kaye, Scholer, *66 S. Cal. L. Rev. 1145 (1993).*

[10] See John P. Heinz & Edward O. Laumann, Chicago Lawyers: The Social Structure of the Bar 319-20 (1982) (finding that the legal profession consists of two categories of lawyers whose practice settings, socioeconomic and ethno-religious backgrounds, education, and clientele differ considerably); John P. Heinz et al., Urban Lawyers: The New Social Structure of the Bar 29-47 (2005) (documenting that lawyers work in two fairly distinct hemispheres - individual and corporate - and that mobility between these hemispheres is relatively limited).

[11] Simshaw, supra note 5, at 550.

[12] Michael McNerney & Emilian Papadopoulos, Hacker's Delight: Law Firm Risk and Liability in the Cyber Age, *62 Am. U. L. Rev. 1243, 1246, 1251 (2013).*

[13] Alan W. Ezekiel, Note, Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft, *26 Harv. J.L. & Tech. 649, 651 (2013).*

might expect large law firms to be relatively well-protected, at least compared to smaller law firms, the payoff for hackers may be worth the investment.

Yet, this is not to suggest that small law firms and solo practitioners who tend to represent small businesses and individual clients [14] are not valuable depositories of client information. Rather, these lawyers may simply feature a different value proposition for hackers. For example, some of their clients may not ordinarily store sensitive information electronically and, thus, may be immune to cyberattacks. Yet, in the context of negotiating a transaction or bringing or defending a lawsuit, such clients are likely to collect information and then send it to their lawyers, who are likely to store it electronically, thus making the latter likely targets for cyberattacks.

Second, compared with their clients, lawyers are assumed to be relatively easy, vulnerable targets for cyberattacks, [15] "perceived to have fewer security resources than their clients, [16] and have less of an understanding of and appreciation for cyber risk." [17] Lawyers' relative cyber vulnerability exposes them not only to attacks seeking confidential client information, but also to hacking designed to disrupt the integrity and availability of information stored by law firms in an attempt to collect ransom payments. [18]

[*506] Once again, attention to context is paramount to the understanding of cyberthreats; whereas lawyers representing large entity clients are likely to be less sophisticated than their clients about cyber risks and have fewer resources and expertise to deal with threats, they nonetheless represent clients who know enough to insist that their law firms take reasonable cybersecurity measures. Lawyers representing small businesses and individuals may know as little as their clients about cyberthreats, but that is no measure of comfort. Not only do such lawyers collect and store their clients' information electronically, exposing it to cyber risk, but they, too, are likely easier targets than their clients who have more to lose and, therefore, a stronger incentive to protect their sensitive information. Worse, small businesses and individuals may erroneously assume that lawyers know enough, or at least more than them about cybersecurity and that their information will be secure with their attorneys. Therefore, they insufficiently inquire and supervise their lawyers' cyber practices.

Finally, the increased competitiveness and ongoing restructuring in the legal profession, both accelerated since the Great Recession, tend to make lawyers especially vulnerable to cyberattacks. Increased competitiveness in the market for legal services has led to the emergence of a dominant "around-the-clock, 24-7" culture of availability to clients. [19] Of course, enhanced lawyer availability is often desirable from the clients' point of view, but when accomplished through mobile remote technology, it enhances cybersecurity risks. [20] Similarly, as competitive pressures lead lawyers to resort to greater use of outsourcing and artificial intelligence, [21] the benefits to clients entail an increased risk of cyberattacks.

---

[14] See supra note 10.

[15] Jane Leclaire & Gregory Keeley, Cybersecurity in Our Digital Lives 128 (2015).

[16] Simshaw, supra note 5, at 550-51.

[17] Leclaire & Keeley, supra note 15, at 128 (2015); Rhodes & Polley, supra note 4, at 105 ("Law firms are viewed as a "very target-rich environment' with significantly less cybersecurity protection in place than their clients have.").

[18] See, e.g., Joe Dysart, "Ransomware' Software Attacks Stymie Law Firms, A.B.A. J. (June 1, 2015, 2:30 AM), *http://www.abajournal.com/magazine/article/ransomware_software_* attacks_stymie_law_firms [*http://perma.cc/M62F-8RT4*].

[19] Eli Wald, Glass-Ceilings and Dead Ends: Professional Ideologies, Gender Stereotypes and the Future of Women Lawyers at Large Law Firms, *78 Fordham L. Rev. 2245, 2264-73 (2010).*

[20] McNerney & Papadopoulos, supra note 12, at 1251.

[21] See, e.g., Milton C. Regan, Jr. & Palmer T. Heenan, Supply Chains and Porous Boundaries: The Disaggregation of Legal Services, *78 Fordham L. Rev. 2137 (2010);* John O. McGinnis & Russell G. Pearce, The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services, *82 Fordham L. Rev. 3041 (2014).*

B. Who Is Attacking the Legal Profession?

All lawyers are susceptible to attacks by malicious insiders, [22] such as disgruntled current and former lawyers and staff members, yet context matters in identifying likely hackers. Large law firms representing large entity clients involved in large-scale **[*507]** transactional work are more likely to be targeted by social engineers, including state-sponsored hackers, [23] and subject to corporate espionage and financial crimes. [24] Smaller law firms, however, while less likely to be attacked by state-sponsored actors, still carry valuable information attractive to social engineers. [25] Government intrusion and surveillance, a growing source of cybersecurity concern for lawyers and their clients alike, [26] may be of particular concern to criminal defense, immigration, and intellectual property lawyers. [27]

C. What Lawyers Can Do About Cyberattacks

Stopping all cyberattacks is impossible to do. Yet, 96% of hacking attacks employ simple techniques, and 97% of attacks can be blocked by common security practices that are within the reach of even small law firms and solo practitioners. [28] These common practices include using current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents, avoiding the use of web-based e-mail services and public Wi-Fi, replacing the default passwords on network hardware, and training employees to recognize deceptive ("phishing") attacks. [29] Beyond these basic measures, defending effectively against cyberattacks entails making decisions about trade-offs between business needs and **[*508]** cybersecurity. [30] For example, is a firm willing to make it more inconvenient for traveling attorneys or lawyers working remotely to access their data, in exchange for more security? When does a business imperative of providing speedy service render certain actions "worth the risk"? [31] Navigating these trade-offs and systematically assessing the cyber risks involved in doing business requires developing and putting in place a comprehensive cybersecurity plan.

---

[22] Simshaw, supra note 5, at 552.

[23] Id.

[24] McNerney & Papadopoulos, supra note 12, at 1264.

[25] Carrie A. Goldberg, Rebooting the Small Law Practice: A Call for Increased Cybersecurity in the Age of Hacks and Digital Attacks, *38 AM. J. Trial Advoc. 519, 521-22 (2015);* see also Noah G. Susskind, Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know, *11 N.Y.U. J.L. & Bus. 573, 579 (2015)* (exploring the vulnerability of smaller companies).

[26] Silkenat, supra note 2, at 456; see also Sarah Jane Hughes, Did the National Security Agency Destroy the Prospects for Confidentiality and Privilege When Lawyers Store Clients' Files in the Cloud - and What, If Anything, Can Lawyers and Law Firms Realistically Do in Response?, ***41 N. Ky. L. Rev. 405, 418 (2014).***

[27] See, e.g., Katie Benner & Eric Lichtblau, U.S. Says It Has Unlocked iPhone Without Apple, N.Y. Times at A1 (Mar. 29, 2016), *http://www.nytimes.com/2016/03/29/* technology/apple-iphone-fbi-justice-department-case.html?_r=0 [*http://perma.cc/4SPB-R96Q*]; Devlin Barrett, Justice Department Seeks to Force Apple to Extract Data from About 12 Other iPhones, Wall St. J. (Feb. 23, 2016), *http://www.wsj.com/article_email/justice-department-seeks-to-force-apple-to-extract-data-from-about-12-other-iphones-1456202213-* lMyQjAxMTI2 MjIzMzMyMTMwWj.

[28] Verizon et al., 2012 Data Breach Investigations Report (2012), *http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf* [*http://perma.cc/GTA4-3DN3*].

[29] Ezekiel, supra note 13, at 649; see also Joel Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare 239-44 (2011).

[30] McNerney & Papadopoulos, supra note 12, at 1265.

[31] Id. at 1265-66.

The first element of a comprehensive cybersecurity plan entails involving firm leadership in learning about cybersecurity threats and making strategic decisions about them. [32] This, to be sure, does not mean that firm executives need to (or can) become cybersecurity experts. It does, however, mean that firm leaders, ranging from members of large law firms' executive committees to solo practitioners managing their own practices, must understand basic cybersecurity realities to allow them to make informed strategic judgments about: what technologies to deploy; how to mine advantages to benefit clients and the practice, and at what costs and risk level; and what security measures to employ. Because putting together a cybersecurity plan calls for strategic decision making that must involve firm management, law firms would be well-advised to task a management-level leader with specific supervisory responsibility for cybersecurity planning.

Second, lawyers must know their data - that is, be cognizant of the actual information the firm possesses and, in particular, be mindful of highly valuable and sensitive information entrusted to firm lawyers, encompassing issues such as what information firm lawyers are working with and how they are using it. Once strategic decisions are made by management, many law firms will likely delegate the implementation of cybersecurity details to non-lawyers, yet lawyer insight and exercise of judgment regarding the nature of client information and its sensitivity must inform the design of cybersecurity plans. For example, a cybersecurity plan may include different levels of protection depending on the circumstances. While a firm may prohibit all **[*509]** lawyers from using public cloud providers, file-sharing services for sharing documents, web-based e-mail services, and public Wi-Fi while conducting firm business, it may demand using cryptographically strong passwords only when receiving or sending highly sensitive client information. A firm may delegate the creation and maintenance of its cybersecurity plan to non-lawyers and may create guidelines for the use of various protections, but ultimately, lawyers would have to be educated to make judgment calls about what measures to use based on their knowledge of their clients' information.

Third, following a strategic, management-level risk analysis of the trade-offs between cybersecurity and business imperatives applied to the actual data a firm possesses, lawyers can then delegate day-to-day operations and implementation authority to technology experts, either within or outside the firm. A large law firm may designate someone internally within its IT department for the task, whereas a solo practitioner or a small firm may hire an outside expert to help manage its security apparatus. Day-to-day implementation of a cybersecurity plan includes two related yet distinct tasks: prevention and breach management. Prevention includes responsibility for deploying secure technologies, restricting access to high-risk activities, and implementing cybersecurity policies and procedures. For example, "blocking malware, [and] detecting anomalous behavior, such as extraction of significant quantities of data off company networks, that can indicate a cyberattack." [33] Perhaps most importantly, it entails training of lawyers and staff to observe cybersecurity practices. [34] The Wall Street Journal reported that "the weakest links at law firms of any size are often their own employees, including lawyers." [35] Having a plan in the event of a data breach, in turn, includes containing an ongoing cyberattack, mitigating its damage, and communicating it to clients. [36]

---

[32] For example, "should the firm be more worried about an attack that disrupts its networks so that attorneys lose access to information, about an attack that reveals sensitive data belonging to clients, or about an attack, that exposes the firm's own secret business data?" Or, "who are the actors that might pursue each of these attacks? What can the company do to prevent each type of attack or, if the attack happens, to manage its consequences?" Id. at 1265; see also Cheryl A. Falvey, Demonstrating Due Diligence in Building an Information Security Program, in Privacy and Surveillance Legal Issues 7 (2014).

[33] McNerney & Papadopoulos, supra note 12, at 1268.

[34] Simshaw, supra note 5, at 568-69.

[35] Jennifer Smith, Lawyers Get Vigilant on Cybersecurity, Wall St. J. (June 26, 2012, 4:09 PM), http://www.wsj.com/articles/SB10001424052702304458604577486761101726748.

[36] See Mercedes Kelley Tunstall, The Path to Comprehensive Cybersecurity Laws in the United States, in Understanding Developments in Cyberspace Law 61, 63 (2015 ed. 2015).

While lawyers in general may delegate to cybersecurity experts the implementation of cybersecurity plans, complex legal ethics questions may arise requiring the insight, approval, and supervision of lawyers. For example, consider the use of honeypots, cybersecurity mechanisms set to detect, deflect, and counteract attempts at unauthorized access to protected **[*510]** information. Generally, honeypots consist of data that appears to be legitimate and thus of value to attackers, but is in fact deceptive information planted to attract hackers who are then tracked and blocked. [37] Among cyber experts, while risky, honeypots are considered a valid information security tactic. [38] Yet, whether law firms can deploy honeypots raises a complicated and unresolved question under the Rules, which generally prohibit lawyers from engaging in dishonest or deceptive practices in the practice of law. [39] Notably, it is a question lawyers need to be made aware of and help resolve.

Finally, law firms must develop a strong culture of cybersecurity, [40] because cyber "compliance and risk management intertwine around corporate culture." [41] Lawyers and staff who think of cybersecurity as somebody else's problem or responsibility are prone to make the very mistakes, like opening phishing e-mails, that expose a firm to heightened risk. Since a law firm's cybersecurity apparatus is only as safe as its weakest link, lawyers and staff must be trained to conceive of cybersecurity not as an imposition on doing business, but as an integral part of firm culture - that is, to move past thinking of business considerations and cybersecurity as a trade-off and accept cybersecurity as a business need. [42]

Context is likely to play an important role in the implementation of cybersecurity plans. Some security measures, indeed, even some basic security measures such as avoiding the use of web-based e-mail services and public Wi-Fi, as well as expensive training, may be out of reach for some solo practitioners and smaller law firms. Yet, as Carrie Goldberg points out, it is in these very types of attorney-client relationships that an attorney is likely to be "more stringent and informed than the client about necessary information security measures." [43] In such instances, a lawyer can enhance the cybersecurity of the attorney-client relationship by explaining to the client the lawyer's limited means and the risks entailed, and communicating the shared responsibility to maintain privacy, **[*511]** especially as it pertains to a client's voluntary online behavior and habits. [44]

II. The Underregulation of Lawyers' Cybersecurity Conduct

Critics from the left and the right have long disparaged professional ideologies, and rules of professional conduct that implement and codify them, as self-serving rhetorical tools meant to justify the profession's power and status, [45] monopoly over the provision of legal services, and anticompetitive fees. [46] At first glance, the recent flurry of

---

[37] See Sean L. Harrington, Cyber Security Active Defense: Playing with Fire or Sound Risk Management? *20 Rich. J.L. & Tech. 12, 14-16 (2014).*

[38] *Id. at 15.*

[39] Model Rules of Prof'l Conduct r. 8.4(c) (Am. Bar Ass'n 2013); see, e.g., *In re Pautler, 47 P.3d 1175 (Colo. 2002)* (disciplining an assistant district attorney who misrepresented himself to a suspected murderer as a public defender); see also *In re Gatti, 8 P.3d 966 (Or. 2000)* (disciplining a lawyer who misrepresented himself as a medical professional in order to obtain information related to the representation of a client).

[40] McNerney & Papadopoulos, supra note 12, at 1266.

[41] Susskind, supra note 25, at 608.

[42] Id. at 608-12.

[43] Goldberg, supra note 25, at 543.

[44] Id.

[45] See, e.g., Richard L. Abel, American Lawyers (1989); Magali S. Larson, The Rise of Professionalism: A Sociological Analysis (1977).

[46] Richard A. Posner, The Problematics of Moral and Legal Theory 185-211 (1999).

changes to Rules regarding cybersecurity [47] appear unnecessary, and thus susceptible to this criticism. To begin with, the Rules have long required lawyers to protect confidential information and so the promulgation of subsection 1.6(c), stating in relevant part that "a lawyer shall make reasonable efforts to prevent the … unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," [48] seems like a redundant clause, a rhetorical nod regarding cybersecurity. Similarly, the Rules have long demanded competence and so the revision of Comment 8 to Rule 1.1, stating in relevant part that "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology … ," [49] seems perfunctory. Moreover, the changes appear unnecessary because on initial consideration one would expect clients' reactions, such as firing a law firm following a security breach, withholding new business, or filing a malpractice lawsuit, to provide lawyers with ample motivation and incentive to reasonably protect clients' information. Cybersecurity thus appears to be the posterchild for advocates of market controls and deregulation; instead of promulgating new rules of professional conduct, let the market regulate lawyers' cybersecurity conduct.

Closer scrutiny, however, reveals that liability rules (e.g., malpractice suits) and market controls (e.g., termination of the attorney-client relationship) are not likely to effectively regulate lawyers' cybersecurity conduct. [50] Generally, a plaintiff in a **[*512]** malpractice lawsuit must establish four elements: the existence of a duty, breach of the duty owed, causation, and damages. [51] Yet a plaintiff in a malpractice suit alleging negligence in failing to protect information is unlikely to be able to prove "damages because of the challenges in answering key questions about cybersecurity breaches: who perpetrated the cyberattack; what information did they steal; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim?" [52] Consequently, there are hardly any cases litigating attorney (or even corporate) negligence for failure to protect confidential information. [53]

The same challenges - not knowing who perpetrated the cyberattack; what information they stole; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim - limit the ability of clients to fire or otherwise sanction a law firm for failing to protect confidential information. Worse, clients are often prevented from reacting to lawyers' cybersecurity inaction because they do not find out about it. To be sure, some clients, usually sophisticated and powerful entity clients, have been pressuring their law firms to put in place cybersecurity measures and others have demanded being advised of security breaches. [54] Yet lawyers are under no general duty to report attacks to clients, [55] often

---

[47] See infra Section III.A.

[48] Model Rules of Prof'l Conduct r. 1.6(c) (Am. Bar Ass'n 2013).

[49] Id. r. 1.1 cmt. 8 (emphasis added).

[50] For a review of disciplinary, liability, institutional, legislative, and market controls, see Wilkins, Who Should Regulate Lawyers?, supra note 9, at 804-19. See generally David B. Wilkins, How Should We Determine Who Should Regulate Lawyers? Managing Conflict and Context in Professional Regulation, *65 Fordham L. Rev. 465 (1996).*

[51] Ronald E. Mallen & Allison Martin Rhodes, Legal Malpractice: The Law Office Guide to Purchasing Legal Malpractice Insurance § 1:2 (2016).

[52] McNerney & Papadopoulos, supra note 12, at 1261.

[53] Id. at 1260; see also Hughes, supra note 26, at 426 ("Most data breach class actions have been dismissed for lack of damages.").

[54] See, e.g., Monica Bay, Understanding the Risks to Cybersecurity: Large Law Firms Are Viewed as Vulnerable and Store Information that Hackers Know Is Valuable, 36 Nat'l L.J. 28, 28 (2014).

[55] See infra Section III.A.

do not learn about attacks themselves, [56] and when lawyers do find out about attacks, they often have insufficient information to allow for comprehensive reporting to clients.

Thus, clients often do not find out about lawyers' cybersecurity breaches, and when they do, they have insufficient information on which to respond or to successfully sue. Unfortunately, underregulation - the inability of clients to effectively utilize liability rules and market controls to ensure that lawyers face appropriate cyber incentives - compounds the **[*513]** underlying problem. As lawyers face insufficient incentives to implement appropriate cybersecurity measures and report attacks to clients, data about attacks and their consequences goes uncollected, diminishing the prospects of effective liability rules and market controls developing in the future. This is the kind of market failure that is unlikely to resolve itself without regulatory intervention, except that liability rules are not likely to constitute an effective regulatory response. It is also the kind of market failure that prevents the collection of the very data we need to better understand the extent of the problem we are facing.

To be sure, underregulation does not mean that lawyers face no regulatory forces pertaining to their cybersecurity conduct. To begin with, legislative controls regulate the cyber conduct of lawyers. State laws impose on lawyers, and others who hold personal information about customers, data breach notification duties if they reasonably believe that an unauthorized party has obtained the customers' information. [57] In addition, various federal statutes address data breach in specific industries. For example, attorneys working in the health care industry who have access to covered information are subject to the privacy and security provisions of the Health Insurance Portability & Accountability Act; [58] other federal statutes generally regulating data security may apply to lawyers as well. [59]

Next, even in the absence of reported malpractice decisions regarding failure to protect confidential client information, liability rules may indirectly inform attorneys' cyber conduct. For example, law firms accused of cybersecurity misconduct by clients may decide to settle cases to avoid having to publicly defend suits risking exposure of embarrassing cyber details and consequential reputational harm. Similarly, market controls may also inform lawyers' conduct, even if clients do not learn about cyberattacks and compromised information. Powerful clients can demand that their lawyers establish reasonable cybersecurity policies, and some lawyers, even in the absence of a duty to disclose information to clients about cyberattacks, may reveal information to build trust in the attorney-client relationship or to avoid undermining it upon subsequent disclosure. Other lawyers may take cybersecurity action to comply with insurance companies' protocols, even if the risk of malpractice liability is remote.

[*514] Yet other lawyers may respond to social norms, such as peer pressure and organically evolving norms within their legal communities. For example, as cybersecurity awareness increases, and Continuing Legal Education providers flood the marketplace with offerings, lawyers may be induced to take a class to keep up with the competition. Also, as younger attorneys, likely more tech-savvy, join the profession, law firms become both more aware of cyber conduct and more apt to engage with it more directly.

In sum, while the ineffectiveness of traditional liability rules and market controls results in the systematic underregulation of lawyers' cybersecurity conduct, other regulatory controls have led to significant changes in the cyber habits of some members of the legal profession, such as the increased use of two-factor authentication in lieu of a single password to access secure systems. [60] Before turning to explore rules of professional conduct as a

---

[56] Simshaw, supra note 5, at 550-51.

[57] McNerney & Papadopoulos, supra note 12, at 1254-55.

[58] Pub. L. No. 104-191, ***110 Stat. 1936 (1996)*** (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

[59] McNerney & Papadopoulos, supra note 12, at 1256 (describing guidelines advising corporations and attorneys to report material cyber risks and incidents to the SEC).

[60] See, e.g., Ellen Blanchard & Rodney Blake, Law Firms Are the New Target for IP Theft: Basic Protections, IPWatchdog (June 19, 2015), *http://www.ipwatchdog.com/* 2015/06/19/law-firms-are-the-new-target-for-ip-theft-basic-protections/ id=58656/ [http://perma.cc/3G3U-9UBY].

possible remedy to lawyers' likely cybersecurity inaction, a word about Holmesian bad people. [61] Since we do not know enough about the extent and scope of cyberattacks against lawyers, admittedly in part because lawyers do not gather or share this information, why assume that lawyers do not do enough to protect their clients' information and best interests? Even conceding a legal world of increased atomism and individualism, one in which lawyers and their clients seek to maximize their short-term interests with little regard to the impact on others, [62] why assume that, but for regulatory intervention, most or even many lawyers will act as Holmesian bad people and try to get away with implementing insufficient cybersecurity measures? Surely some lawyers will do the right thing by their clients simply because it is the right thing to do.

Regrettably, in addition to the dominance of individualism (or the hired gun ideology) [63] and the relative decline of relational approaches in legal (and business) decision making made by both clients and lawyers, [64] three interrelated reasons suggest that, **[*515]** absent regulatory intervention, some lawyers are likely to try to get away with offering insufficient cyber protection to clients and acting as Holmesian bad people.

First, implementing effective cybersecurity measures can entail significant expenses. While some costs can be easily rolled onto clients, for example, expenses directly related to undertaking specific measures in connection with the representation of clients with known security risks and needs, other expenses, such as the cost of upgrading the entire cybersecurity apparatus of the firm or the time investment of lawyers and staff learning about the apparatus, may be harder to recoup.

Second, even when the costs of implementing cybersecurity measures can be recouped, lawyers are notoriously technophobic. [65] To be sure, some lawyers are at the forefront of using new technological advances to better serve clients. [66] Yet the legal profession has a long, documented history of resisting technological advances due to ignorance, [67] vanity, [68] status envy, [69] and independence, [70] which suggests that, left to their own devices, lawyers are unlikely to implement the necessary cybersecurity measures to protect clients' information.

Finally, some cybersecurity measures, such as limiting access to unsecure networks and mobile devices, abstaining from using portable drives, frequent change of passwords, and timely lock down of computers in and out of the office, are likely to be perceived to be, and indeed are, cumbersome for lawyers. This is especially true for older and less technology-savvy attorneys, some of whom, by virtue of their seniority, are also likely to be powerful

---

[61] See Russell G. Pearce & Eli Wald, Rethinking Lawyer Regulation: How a Relational Approach Would Improve Professional Rules and Roles, *2012 Mich. St. L. Rev. 513, 522-23 (2012).*

[62] See Russell G. Pearce & Eli Wald, The Obligation of Lawyers to Heal Civic Culture: Confronting the Ordeal of Incivility in the Practice of Law, *34 U. Ark. Little Rock L. Rev. 1, 26-39 (2011).*

[63] See generally William H. Simon, The Ideology of Advocacy: Procedural Justice and Professional Ethics, 1978 Wis. L. Rev. 29 (1978).

[64] Pearce & Wald, supra note 62; Russell G. Pearce & Eli Wald, The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law, *42 Hofstra L. Rev. 109, 110 (2013).*

[65] Timothy J. Toohey, Beyond Technophobia: Lawyers' Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks, *21 Rich. J.L. & Tech. 9 (2015).*

[66] See William Henderson, What the Jobs Are: New Tech and Client Needs Create a New Field of Legal Operations, A.B.A. J. (Oct. 1, 2015, 6:00 AM), *http://www.abajournal.com/* magazine/article/what_the_jobs_are [*http://perma.cc/WHB9-E4UC*].

[67] See, e.g., Brian E. Finch, The Legal Profession Needs to Get Smart About Cybersecurity, Nat'l L.J. 27, at 27 (2015).

[68] Vivia Chen, Why is "Phooling' a Lawyer So Easy?, Nat'l L.J. 5, at 5 (2015).

[69] Ezekiel, supra note 13, at 656.

[70] Id.

within their firms and therefore harder to reign in. In sum, because liability rules and market controls are unlikely to provide lawyers with a sufficient incentive to take appropriate cybersecurity action, and because implementing effective cybersecurity measures is expensive, time-consuming, and inconvenient, some lawyers are unlikely to reasonably protect their clients' information absent regulatory intervention.

[*516]

III. The Legal Ethics of Cybersecurity

Professional ideologies and rules of professional conduct promulgated by lawyers are often self-serving and warrant a healthy dose of skepticism, yet at the same time, they play an important and effective role in the regulation of lawyers. As liability rules, the rules of professional conduct - part and parcel of state law - define misconduct and give rise to a disciplinary system that incentivizes lawyers to comply with them. [71] As the embodiment of professionalism, rules of professional conduct are social norms that shape and guide the conduct of lawyers. Thus, notwithstanding criticisms of rules of professional conduct and acknowledging their chronic underenforcement, [72] legal ethics rules can play an important role in the regulation of lawyers. [73]

A. The Current Legal Ethics Stance on Cybersecurity

To their credit, the Rules have been revised in recent years to take account of technological changes impacting the practice of law. In August 2012, the ABA House of Delegates renumbered Comment 6 to Rule 1.1 on competence as Comment 8 and added a clause calling on lawyers to keep abreast of relevant technology affecting their practice. While the revision was made to a Comment rather than in the body of the Rule, was aspirational rather than mandatory, and failed to explicitly identify cybersecurity as a concern or a priority (stating instead that "to maintain the requisite knowledge and skill" mandated by Rule 1.1, "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology ..."), [74] the Comment revision was not without practical impact. It does open the door to discipline, designating ignorance of relevant technology as incompetence and thus misconduct, and, by identifying knowledge of relevant technology as a component of competence, it did help give rise to a cottage industry of Continuing Legal Education courses about cybersecurity. [75] Notably, however, the Comment does not deem **[*517]** the failure to utilize technology or inaction with regard to technological risks as incompetent conduct. Rather, all it recommends is keeping abreast of benefits and risks of relevant technology.

Arguably, a more significant change was made to Rule 1.6 on confidentiality. Elevating a Comment to a new subsection of Rule, 1.6(c), the Rule now mandates that "[a] lawyer shall make reasonable efforts to prevent … the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." [76] Importantly, exactly because the dearth of malpractice litigation regarding failure to protect information results in

---

[71] Model Rules of Prof'l Conduct r. 8.4(a) (Am. Bar Ass'n 2013). Rules of professional conduct also establish standards of conduct which inform determination of civil liability for malpractice. See id. at Preamble & Scope P 20.

[72] Richard L. Abel, Why Does the ABA Promulgate Ethical Rules?, 59 Tex. L. Rev. 639, 648 (1981) ("Study after study has shown that the current rules of professional conduct are not enforced."); Wilkins, Legal Realism for Lawyers, supra note 9, at 493 (noting that the rules of professional conduct tend to be "systematically underenforced").

[73] Richard H. McAdams, The Origin, Development, and Regulation of Norms, *96 Mich. L. Rev. 338 (1997)* (discussing how legal norms and rules affect professional conduct).

[74] Model Rules of Prof'l Conduct r. 1.1 cmt. 8 (emphasis added).

[75] Darla W. Jackson, Cybersecurity: Breaches and Heartbleed to BYOD - Are Bankers, Entertainment Company Executives, Celebrities, Postal Workers, Ice Cream Lovers, Home Builders, and CIOs the Only Ones Who Should Be Concerned?, ***106 L. Libr. J. 633, 638 (2014)*** (noting that the A.B.A. has begun offering a Cybersecurity Series); see also ABA Cybersecurity Series, A.B.A., *http://www.americanbar.org/content/ebus/events/ce/cyber-security-core-curriculum.html* [*http://perma.cc/6X3H-LN49*].

[76] Model Rules of Prof'l Conduct r. 1.6(c) (emphasis added).

lack of judicial exposition of reasonableness, new Comments 18 and 19 to Rule 1.6 do offer a partial definition of reasonable efforts.

After emphasizing the central role of reasonableness, stating that "the unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure," [77] Comment 18 adds that:

factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). [78]

Comment 19 similarly identifies reasonableness as a key term of art, adding that "when transmitting a communication that includes information relating to the representation of a client," [79] that is, confidential information, [80]

the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients … . Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. [81]

[*518] Comments 18 and 19 take a first important step in defining the meaning of "reasonable efforts" to protect clients' information. They correctly identify reasonableness as a key element in assessing cybersecurity measures, and they begin to define the term, referring to the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients as relevant considerations of reasonableness.

Yet Rule 1.6(c) and Comments 18 and 19 fall short in several respects. First, they fail to require that lawyers put in place a cybersecurity plan which will regularly monitor their cybertechnology to detect breaches. Perhaps the Comment implies a duty to regularly monitor one's cybersecurity measures, after all, how can a lawyer assess "the likelihood of disclosure if additional safeguards are not employed" without monitoring the performance of existing safeguards? Similarly, assessing "the cost of employing additional safeguards" as well as "the difficulty of implementing the safeguards" implies a duty to assess one's existing apparatus. But the Comments fail to explicitly identify a duty to implement a cybersecurity plan, a noteworthy omission given that elsewhere the Comments do explicitly impose similar duties. For example, while a duty to monitor for conflicts of interest may be implied from a Rule prohibiting conflicts of interest, Comment 3 to Rule 1.7 on conflicts of interest explicitly states that:

to determine whether a conflict of interest exists, a lawyer should adopt reasonable procedures, appropriate for the size and type of firm and practice, to determine … the persons and issues involved … . Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule. [82]

---

[77] Id. r. 1.6 cmt. 18.

[78] Id.

[79] Id. r. 1.6 cmt. 19.

[80] Id. r. 1.6(a).

[81] Id. r. 1.6 cmt. 19 (emphasis added).

[82] Id. r. 1.7 cmt. 3.

Yet, while ignorance about cybersecurity attacks and their scope appears to be the norm, the Comment to Rule 1.6 fails to explicitly demand monitoring for cyberattacks akin to the monitoring of conflicts of interest.

Second, Rule 1.6(c) and its Comment do not sufficiently clarify what constitutes "reasonable efforts" and "reasonable precautions." Perhaps, in a world of constantly evolving technology, the Comment avoided specifying the nature of appropriate measures to prevent it from quickly becoming antiquated. Curiously, however, the Comment did not shy away **[*519]** from delving into the meaning of reasonableness when such analysis benefited lawyers. Comment 19 states in relevant part that "this duty," to take reasonable precautions to prevent the unauthorized disclosure of client information, "however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy." [83] This innocent sounding clause implicitly refers to ABA Formal Opinion 99-413, in which the ABA Standing Committee held that "[a] lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the [Rules] because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint." [84]

In other words, Comment 19, while ostensibly staying clear of defining the meaning of "reasonable efforts," nonetheless states that the use of unencrypted e-mail by lawyers is reasonable because apparently unencrypted e-mails "afford[] a reasonable expectation of privacy" based on Formal Opinion 99-413, which found that "the same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail." [85] The point, to be clear, is not to debate whether the Committee's conclusion, made in 1999, that unencrypted e-mails afford a reasonable expectation of privacy, still holds true presently, although some have characterized the conclusion as "misguided." [86] Rather, it is that what Comment 19 does half-heartedly and indirectly [87] - delving into the definition of reasonable efforts - it ought to do openly and clearly.

Third, Rule 1.6(c) and its Comment fails to mandate disclosure to clients regarding cyberattacks and/or security breaches regarding client information. There are at least two possible good faith explanations for this omission. To begin with, attorney-client communications are generally governed by Rule 1.4, not Rule 1.6, and so there would be no reason to require communications regarding cybersecurity in the latter. Yet the **[*520]** Rules and Comments often explicitly cross-reference other Rules such that the failure to reference Rule 1.4 is glaring. Indeed, Comment 18 does reference Rules 1.1, 5.1, and 5.3, making the omission to reference Rule 1.4 inexplicable. Next, Comments 18 and 19 do implicitly reference Rule 1.4, both stating in relevant part that "[a] client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule." [88] Rule 1.4(a)(1), in turn, states in relevant part that "[a] lawyer shall promptly inform the client of any decision or circumstance with respect to which the client's informed consent … is required," [89] such that one could argue that the Comments 18 and 19 indirectly reference Rule 1.4 (by referring to informed consent, which requires communicating with clients). But even viewed in the light most favorable to the Rules, such indirect reference to Rule 1.4 is lacking as it fails to require disclosure to clients of cybersecurity attacks or breaches. It only indirectly triggers a duty to communicate regarding forgoing security

---

[83] Id. r. 1.6 cmt. 19.

[84] A.B.A. Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (discussing protection of confidentiality by means of unencrypted e-mail).

[85] Id.

[86] Toohey, supra note 65, at 23; see also Rebecca Bolin, Risky Mail: Concerns in Confidential Attorney-Client Email, *81 U. CIN. L. REV. 601, 618-21 (2012)* (discussing and critiquing the effect of 99-413).

[87] Curiously, Comment 19 fails to identify Formal Opinion 99-413, although it appears to cite its language. Compare Model Rules of Prof'l Conduct r. 1.6 cmt. 19 (Am. Bar Ass'n 2013), with ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

[88] Model Rules of Prof'l Conduct r. 1.6 cmt. 18.

[89] Id. r. 1.4(a)(1).

measures as opposed to imposing a general duty to communicate regarding cybersecurity. Furthermore, Comments 18 and 19 fail to reference the subsections of Rule 1.4 that may give rise to a duty to communicate regarding cybersecurity concerns, namely 1.4(a)(2), 1.4(a)(3), and 1.4(b).

Notwithstanding the silence of Rule 1.6(c), does Rule 1.4 independently require lawyers to communicate with clients regarding cybersecurity, let alone advise clients about cyberattacks against the law firm and/or breaches of security? Most commentators opining on this issue believe the Rules do not impose such a duty, [90] and regrettably they appear to be right because the Rules essentially only mandate disclosure of material information to clients, and the usual uncertainty engulfing cyberattacks casts an inherent doubt on the materiality of cyberattacks and resulting breaches.

Rule 1.4(a)(2) states that "[a] lawyer shall … reasonably consult with the client about the means by which the client's objectives are to be accomplished." [91] Cybersecurity measures certainly qualify as part of the means by which the client's objectives are to be accomplished, and thus would support an interpretation pursuant to which a lawyer must reasonably **[*521]** consult with the client about reasonable security measures, for example, whether to encrypt communications regarding the representation, but the Rule falls short of explicitly demanding such a communication. Therefore, if a lawyer has in place cybersecurity measures, or reasonably believes that his cybersecurity measures or lack thereof are sufficient, Rule 1.4(a)(2) does not appear to require any communication whatsoever. Worse, Rule 1.4(a)(2) says nothing whatsoever about cyberattacks or security breaches.

Rule 1.4(a)(3) states that "[a] lawyer shall keep the client reasonably informed about the status of the matter," [92] and Comment 3 adds that "paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation." [93] If cybersecurity measures are to be construed as the "means by which the client's objectives are to be accomplished," they are certainly not the matter, and thus, 1.4(a)(3) appears not to generally apply to cybersecurity communications. However, a significant cybersecurity breach that results in the disclosure of otherwise confidential and privileged information, or that foils the negotiation of a transaction on behalf of a client, can certainly impact the status of a matter. Comment 3 supports that interpretation because a significant cybersecurity breach would be a "significant development" affecting the substance of the representation. [94]

In any event, however, Rule 1.4(a)(3) falls short of imposing a general duty of communication regarding cybersecurity attacks and breaches. Rather, it only mandates disclosure to clients of significant cyber breaches which constitute a significant development and result in an impact regarding the status of the representation. Moreover, the same considerations that obscure clients' ability to prove damages resulting from a lawyer's failure to reasonably protect information - not knowing who perpetrated the cyberattack, what information they stole, what the value of that information is to them or others, and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim - would often shield lawyers from discipline for violating 1.4(a)(3). If a lawyer does not know who perpetrated the cyberattack, what information was stolen, what the value of that information is to them or others, and what other **[*522]** harms resulted for the client, how could a lawyer ever conclude that a breach constitutes a "significant development"?

---

[90] See, e.g., Ezekiel, supra note 13, at 653 ("Most astonishingly, the existing professional responsibility standards generally do not require any disclosure to the client when client information is stolen from a law firm.").

[91] Model Rules of Prof'l Conduct r. 1.4(a)(2).

[92] Id. r. 1.4(a)(3).

[93] Id. r. 1.4 cmt. 3.

[94] See Colo. Bar Ass'n Ethics Comm., Formal Ethics Op. 113 (Nov. 19, 2005) (discussing the ethical duties of an attorney to disclose errors to a client).

Rule 1.4(b) states that "[a] lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." [95] While Rule 1.4(b) appears to only apply to explaining the "matter" at hand, Comment 5 importantly clarifies that:

the client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued … . The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation. [96]

Rule 1.4(b) arguably gives rise to a general duty to communicate regarding cybersecurity and, in particular, about cyberattacks and breaches because cybersecurity measures are part of the means by which the client's objectives are to be pursued. Thus, the client should receive sufficient information from the lawyer to be able to participate intelligently in decisions concerning cybersecurity. ABA Formal Opinion 95-398 lends support to this interpretation, finding that "should a significant breach of confidentiality occur … a lawyer may be obligated to disclose such breach to the client or clients whose information has been revealed," [97] citing Rule 1.4(b), and adding that "where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b)." [98] Yet, like Rule 1.4(a)(3), the communication appears to be mandated only with regard to severe cyberattacks with significant impact on a client, or limited to communications regarding cybersecurity "means" rather than a clear general duty requiring communication regarding cybersecurity measures, attacks, and breaches. [99]

Some commentators have argued that Rule 1.15 on safekeeping property pertains to protecting client information because Rule 1.15(a) states, inter alia, that "other property," presumably including information, "shall be … appropriately safeguarded." [100] No doubt Rule 1.15 applies, if only to impose on lawyers a duty to monitor client trust accounts for cyberattacks **[*523]** and breaches. [101] Yet, the application adds little to Rules 1.6(a) and 1.6(c), which impose a general duty to protect clients' confidential information from unauthorized disclosure.

Rule 5.1, regarding responsibilities of supervisory lawyers to other lawyers, and Rule 5.3, regarding supervisory responsibilities to non-lawyer assistance, have been slightly revised to reflect technological changes. Read together, Rules 5.1 and 5.3 require some lawyers to supervise the conduct of other lawyers and non-lawyers inside and outside of the practice. They state that supervisory lawyers "shall make reasonable efforts to ensure that the

---

[95] Model Rules of Prof'l Conduct r. 1.4(b).

[96] Id. r. 1.4 cmt. 5 (emphasis added).

[97] ABA Comm. on Ethics & Prof'l Resp., Formal Op. 95-398 (1995).

[98] Id.; see also N.H. Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013), *https://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp* ("Where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent."); Pa. Bar Assoc., Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011),*http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf* [*http://perma.cc/GJ87-T8TS*] ("While it is not necessary to communicate every minute detail of a client's representation, "adequate information' should be provided to the client so that the client understands the nature of the representation and "material risks' inherent in an attorney's methods.").

[99] See also Alaska Rule 5.3(d) (2014), dictating that "[a] lawyer who learns that any person employed by the lawyer has revealed a confidence … protected by these rules shall notify the person whose confidence or secret was revealed." Importantly, however, the rule does not generally apply to a law firm experiencing a cyberattack and compromised information but rather only to a third party employed by the law firm.

[100] Model Rules of Prof'l Conduct r. 1.15(a); see also Goldberg, supra note 25, at 529-30; Hughes, supra note 26, at 415-16.

[101] Christine Daleiden, Information Security Basics for Lawyers, 18 Haw. B.J. 4, 8-9 (2014).

firm has in effect measures giving reasonable assurance that," [102] first, "all lawyers in the firm conform to the Rules of Professional Conduct," [103] including Rules, such as 1.1 and 1.6 pertaining to cybersecurity, and second, that the conduct of non-lawyers employed by, retained by, or associated with the lawyer, "is compatible with the professional obligations of the lawyer." [104] As one commentator notes:

These rules reflect the notion that a law firm's data security practices are only as strong as its weakest link. As a result, lawyers must make sure that subordinate attorneys, interns, paralegals, case managers, administrative assistants, and external business partners all understand necessary data security practices and the critical role that all parties play in ensuring the protection of client information. [105]

In addition, these changes make modest positive contributions to lawyers' understanding of new technological realities. For example, the title of Rule 5.3 was changed from **[*524]** "Responsibilities Regarding Nonlawyer Assistants," to "Responsibilities Regarding Nonlawyer Assistance," to capture the notion that technology, including cybertechnology, assists lawyers in the practice of law. Rule 5.3, providing examples of the use of non-lawyers outside the firm, offers "using an Internet-based service to store client information" as an illustration. [106]

Yet, Rules 5.1 and 5.3, once again, forgo an opportunity to take a clear detailed stance regarding cybersecurity efforts and measures. For example, Comment 2 on Rule 5.1 states that "paragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules," [107] and goes on to give examples of such "internal policies and procedures," a perfect opportunity to require cybersecurity measures, including the adoption of cybersecurity plans. Instead, it states "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised." [108]

Similarly, while Comment 3 on Rule 5.3 identifies lawyers' use of cloud computing as a form of non-lawyer assistance, it fails to detail any of the efforts and measures lawyers must employ in conjunction with the use of this technology. Instead, it generically states that: "when using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations," adding that "the extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; [and] the terms of any arrangements concerning the protection of client information." [109] In other words, the Rules once again invoke reasonableness without specifying its content and a commitment to protecting confidentiality without specific guidance as to the cybersecurity measures lawyers must put in place.

Lawyers' use of cloud computing has been the subject of various ethics opinions that serve as a revealing example of how **[*525]** ethics committees follow the lead of the Rules and offer only a limited insight into the meaning of reasonableness. Ethics opinions generally hold that cloud computing is permissible, as long as lawyers take

---

[102] Model Rules of Prof'l Conduct r. 5.1.

[103] Id.

[104] Id. r. 5.3.

[105] Simshaw, supra note 5, at 563.

[106] Model Rules of Prof'l Conduct r. 5.3 cmt. 3.

[107] Id. r. 5.1 cmt. 2.

[108] Id. Arguably, given Rule 1.15's requirement that lawyers protect clients' property, including clients' trust accounts, Comment 2 could be read to demand cybersecurity measures to protect such accounts, but this would be at best an implied requirement.

[109] Id. r. 5.3 cmt. 3.

reasonable steps when selecting and using services. [110] Notably, some states appear to impose additional, specific cybersecurity measures (Iowa requires lawyers to "determine the degree of protection the vendor provides to its clients' data"; New Jersey requires lawyers to "make sure that vendors are using available technology to guard against foreseeable infiltration attempts"; and North Carolina demands that its lawyers "evaluate the vendor's security and backup strategy"), and The ABA Cybersecurity Handbook wisely acknowledges that "lawyers should monitor and reassess the protections of the cloud provider as the technology evolves." [111] How lawyers are to go about meeting these requirements, however, is less than clear. As Drew Simshaw points out, "it is also worth noting the limits of a lawyer's duties under the rules," [112] according to these ethics opinions. For example, in New Hampshire, "a lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology," and "when it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard." [113]

All in all, the ABA must be commended for its proactive approach to addressing the evolving impact of technology on law practice. New subsection 1.6(c) explicitly identifies protection of client information, including cybersecurity measures, as a priority, and moving the language from a Comment to the body of the Rules signifies to lawyers the emphasis the Rules now place on information protection. [114] Next, the new subsection takes a first important step in shifting lawyers' focus from avoiding **[*526]** negligent and inadvertent disclosure to the new landscape of affirmatively protecting client information from unauthorized access by third parties. Moreover, Comments 18 and 19 to Rule 1.6 help clarify the meaning of the duty to protect client information by specifying the factors that render protective measures reasonable. Appropriate references to this new approach are made in Rules 1.1, 1.15, 5.1, and 5.3. Yet the Rules do not do enough to guide lawyers' cybersecurity conduct, especially given that liability rules and market controls are not likely to incentivize lawyers to sufficiently protect client information.

B. Responding to the New Frontier: The Future of Legal Ethics in the Age of Hackers and Cyberthreats to Clients' Information

The Rules embody, and have long taken, a one-size-fits-all, universal approach to the regulation of lawyers' conduct. [115] As such, they cannot, and should not, be amended frequently to reflect minor changes in the practice of law. Rather, the Rules are open-ended standards that can and should accommodate practice changes, for example via clarifying formal ethics opinions. However, sometimes changing practice realities do necessitate revisions to the Rules, and in such circumstances the Rules must be revised so they can continue to inform and guide lawyers' actual practice and avoid becoming antiquated. [116]

---

[110] Cloud Ethics Opinions Around the U.S., A.B.A., *http://www.americanbar.org/* groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloudethics-chart.html [*http://perma.cc/VY84-VA7P*]. In addition, The ABA Cybersecurity Handbook contains an appendix of "Ethics Opinions on Lawyer Confidentiality Obligations Concerning Cloud Computing." Rhodes & Polley, supra note 4, at 245.

[111] Id. at 77.

[112] Simshaw, supra note 5, at 565.

[113] N.H. Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013), supra note 98.

[114] For an excellent analysis of the Rules' new approach to cybersecurity, see generally Judith L. Maute, Facing 21st Century Realities, *32 Miss. C. L. Rev. 345 (2013).* The ABA has tried to stay at the forefront of enhancing lawyers' cybersecurity awareness. For example, in April 2016, ABA President Paulette Brown offered ABA members an opportunity to receive FBI cybersecurity alerts, noting that, "the ABA is keenly aware of the increase in efforts to hack into the computer systems of legal professionals to reach the significant amounts of non-public information they hold." See E-mail from Paulette Brown, President, Am. Bar Ass'n, to ABA Members (Apr. 12, 2016, 2:00 AM) (on file with author).

[115] Wald, supra note 9, at 228.

[116] Id.

Cybersecurity is one such instance that necessitates changing the Rules. Protecting confidential client information, a fundamental tenet of law practice, used to be about avoiding negligent inadvertent disclosure. Typical examples of misconduct were leaving one's notes or laptop unattended in a conference room, or inadvertently disclosing confidential information to opposing counsel over e-mail. [117] Hackers, however, present a different challenge, one of affirmatively protecting information from unauthorized preying parties, often engaged in criminal activity. Technological advances commonly utilized in the practice of law, and the risks to unauthorized disclosure of client information they entail, thus require a regulatory shift in the Rules, from avoiding inadvertent disclosure to acknowledging a positive duty to protect confidential information. Put differently, the unique challenge cybersecurity concerns present is not merely coming to terms with technological advancements, which **[*527]** the profession, while reluctant, has done in the past. [118] Rather, it is shifting from a passive regime of avoiding negligent disclosure to an active regime of affirmatively protecting information against parties, some of which engage in criminal activity.

To be clear, the emergence of lawyers' affirmative duty to reasonably protect client information from unauthorized disclosure is not a move toward strict liability. Fully protecting client information from all cyberattacks is not feasible given current available technologies, and even if complete protection was possible, it might so undercut the use of effective technology and be so cost prohibitive as to render it unreasonable. Furthermore, utilizing technology to better serve the needs of clients, and confronting the risks inherent in the use of technology, is and ought to be a joint attorney-client undertaking. As clients reap the benefits of new technologies and are sometimes better positioned as compared to their lawyers to address their risks, there is no reason to impose strict liability on lawyers for the use of technology in the practice of law. Accordingly, lawyers need only take reasonable steps to protect client information. Yet, the Rules' approach to cybersecurity must recognize and effectuate an affirmative duty to reasonably protect clients' information and develop a helpful definition of reasonableness that encompasses an obligation to protect client information from criminal activity. The Rules must clarify that a lawyer not only needs to avoid negligently leaving notes in plain view, but must also protect against theft of one's virtual briefcase.

1. Mandating the Adoption of Appropriate Cybersecurity Plans for All Clients

Lawyers' cybersecurity conduct is underregulated, which likely results in insufficient action to protect client information. Because liability rules and market controls are unlikely to effectively incentivize lawyers to take reasonable action, the Rules must require that lawyers adopt appropriate cybersecurity plans. Revealingly, the ABA's Resolution 109 "encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected." [119] Yet nothing in the Rules imposes a duty on lawyers to develop cybersecurity programs for all clients.

[*528] To be sure, Comment 18 on Rule 1.6 does state that: "paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties," and adds that: "the unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure," [120] arguably indirectly encouraging lawyers to put in place a cybersecurity plan for all clients. After all, "acting competently" and making "reasonable efforts" would seem to require at least implementing a cybersecurity plan. Yet the Rules do not affirmatively require the adoption of such a plan and would appear to tolerate an interpretation that at least in some circumstances the prongs of "acting competently" and

---

[117] Silkenat, supra note 2, at 450; see, e.g., Model Rules of Prof'l Conduct r. 4.4(b) (Am. Bar Ass'n 2013).

[118] Toohey, supra note 65.

[119] ABA Cybersecurity Resolution, supra note 3 (emphasis added).

[120] Model Rules of Prof'l Conduct r. 1.6 cmt. 18.

making "reasonable efforts" could be satisfied without the implementation of a cybersecurity plan. Indeed, Comment 18 does not specify what constitutes "acting competently" nor "reasonable efforts." [121]

The Rules ought to require that all lawyers maintain an appropriate cybersecurity plan, akin to Comment 3 on Rule 1.7, which mandates the adoption of reasonable conflict-checking procedures. [122] Accordingly, a new Comment X to Rule 1.6 should read:

to competently safeguard information relating to the representation of a client against unauthorized access by third parties, a lawyer must adopt reasonable procedures, including reasonable cybersecurity measures, appropriate for the size and type of firm and practice, to protect a client's confidential information. Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule. [123]

[*529]

2. Defining "Reasonable Efforts": Reasonable Cybersecurity Measures

Just as Comment 3 on Rule 1.7 has resulted in virtually all law firms employing a conflict-checking software as the first step in detecting conflicts of interest, proposed new Comment X to Rule 1.6 should result in all law firms adopting basic cybersecurity measures, such as employing current virus scanners and firewalls, installing patches and updates, and using cryptographically strong passwords, reasonably replaced from time to time, [124] as the first step in implementing a comprehensive cybersecurity plan. Yet the adoption of basic cybersecurity measures should not be left to chance. Instead, adoption of such basic security measures must be explicitly recognized as a professional requirement for any attorney who stores sensitive client data on an Internet-connected computer. [125] For example, law firms must be expected to demonstrate their system's ability to detect and repel a cyberattack. [126]

Thus, to begin with, "reasonable efforts" must include basic cybersecurity measures such as "robust strategies for identifying, prioritizing, and securing … valuable information," [127] periodical inspection of the firm's operating and information storage systems for signs of cyberattacks and data theft, the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents, avoiding the use of web-based e-mail services and public Wi-Fi, replacing the default passwords on network hardware, and the adoption of training protocol for firm lawyers and staff, appropriate for the size and practice of the firm, for example, to recognize phishing attacks. [128]

A new Comment Y to Rule 1.6 should read:

---

[121] See Ezekiel, supra note 13, at 658-59 ("These rules generally require the law firms to take "reasonable efforts,' "reasonable steps,' or "reasonable precautions' to avoid unauthorized disclosure, but are unspecific about what such precautions might entail. One rule demands that the precautions taken must "meet[] industry standards," but is unfortunately vague about whether it refers to the standards of the legal industry or those of the Internet data storage industry.") (internal citations omitted).

[122] Model Rules of Prof'l Conduct r. 1.7 cmt. 3.

[123] The Comment to Rule 1.6 includes two sections, Comments 18 and 19, under the subheadings of "Acting Competently to Preserve Confidentiality." See id. The proposed Comment can be added as Comment 18, renumbering current Comments 18 and 19 as 19 and 20 respectively; or as Comment 20 (renumbering current Comment 20 regarding confidentiality duties owed to former clients as Comment 21). Or the proposed Comment can be added to the existing Comment. For a redline of the proposed revisions to the Rules, see Appendix A.

[124] See supra note 29 and accompanying text.

[125] See Ezekiel, supra note 13, at 665.

[126] Silkenat, supra note 2, at 455.

[127] McNerney & Papadopoulos, supra note 12, at 1250.

[128] See supra note 29 and accompanying text.

reasonable efforts to prevent the inadvertent or unauthorized disclosure of electronically stored information relating to the representation of a client would normally include robust strategies for identifying, prioritizing, and securing valuable information; periodical inspection of the firm's information storage system for signs of cyberattacks and data theft; the use of basic cybersecurity measures, including the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords **[*530]** updated from time to time, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents; and the adoption of cybersecurity training protocols for firm lawyers and staff. See Rule 5.1 and 5.3. [129]

An attempt to identify basic cybersecurity measures in the Comment entails two related risks. A closed-list of measures may, over time, be treated as a "check-a-box" procedure for purposes of avoiding discipline, or understood to constitute a safe harbor - in the sense that lawyers who employ these basic cybersecurity measures may never be found to have failed to make "reasonable efforts" to protect their clients' information. To avoid such misapprehension, the Comment should explain that basic cybersecurity measures form but a floor for appropriate cyber conduct, necessary but often insufficient means of satisfying the requirement of "reasonable efforts." Far from constituting a safe harbor, basic measures simply set up a default foundation for "reasonable efforts," which depend on a variety of factors already identified by the Comment. Moreover, the Comment should explicitly state that some circumstances may require the adoption of additional special cybersecurity measures.

Comment Z to Rule 1.6 may accordingly add that:

whether a lawyer may be required to take additional special security measures to safeguard a client's information, above and beyond basic cybersecurity measures, depends on the circumstances. For example, a lawyer may be required to take special security measures to protect sensitive information related to the representation of a client. [130]

Relatedly, technological advances may, over time, render proposed Comment Y obsolete, a concern compounded by the traditional delay involved in adoption of revisions to the Rules, first at the ABA level and subsequently by states to their respective rules of professional conduct. Indeed, one commentator concludes that given the long delay inherent in Rules revisions, the "ABA and state bar associations have demonstrated that they might not be the best sources of reform in this subject [cybersecurity]." [131] Yet one should not overstate the rate of relevant technological advances, indeed, many of the currently available basic cybersecurity measures, admittedly in more **[*531]** primitive forms, have been available for a few decades now. In any event, lamentable delays in promulgation and revision notwithstanding, the Rules remain the only practical and, therefore, most operative means of correcting for the underregulation of lawyers' cybersecurity conduct, given the ineffectiveness of liability rules and market controls and the distant probability of national cybersecurity legislation, let alone one that would apply to lawyers. If at all, a years-long delay in the promulgation of the Rules and their adoption by the states does not constitute a compelling reason to avoid regulation. Quite the contrary, the delay ought to be addressed by reforming the historical process of promulgation and adoption to ensure that the Rules remain relevant and helpful to lawyers. There is no denying that old political habits die hard, especially at the hands of the ABA House of Delegates and state supreme courts' advisory committees. Yet, failure by the legal profession to effectively regulate itself may result, and in fact has resulted, in increased federal and state legislation undermining the profession's privilege of self-regulation. [132]

---

[129] See infra Appendix A for a redline of the proposed revisions to the Rules. Rules 5.1 and 5.3 ought to be amended respectively to reference proposed Comment Y to Rule 1.6.

[130] Id.

[131] Travis Andrews, Technological Innovation, The Legal Profession and the Need for Uniform Law, Charlotte L. Rev. (forthcoming 2016) (manuscript at 2), http://papers.ssrn.com/ sol3/papers.cfm?abstract_id=2684950.

[132] See Daniel R. Coquillette & Judith A. McMorrow, Zacharias's Prophecy: The Federalization of Legal Ethics, 48 San Diego L. Rev. 123 (2011) (documenting the federalization of legal ethics); Bruce A. Green, ABA Ethics Reform from "MDP" to "20/20":

Nor would an ABA Formal Opinion be an adequate substitute to proposed Comment Y to Rule 1.6. Ethics opinions, while relatively easier and faster to publish and withdraw, if rendered obsolete, have no binding authority and are therefore inferior to Rules' revisions. [133] Moreover, given the underregulation of lawyer's cybersecurity conduct, ethics opinions will simply not do. The Rules must be revised to send lawyers a credible message, both substantively and symbolically, about the importance of acting affirmatively to protect clients' information. If technology ends up rendering proposed Comment Y obsolete, it can be revised in accordance with evolving cybersecurity knowledge and expertise.

[*532]

3.

"Reasonable Efforts" Further Construed

To further clarify that basic cybersecurity measures merely define a floor rather than a ceiling for "reasonable efforts," the Comment to Rule 1.6 must spell out the meaning of "reasonable efforts" beyond such basic steps. Comment 18 already helps construe "reasonable efforts," stating in relevant part:

factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). [134]

Comment 19 adds that:

when transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. [135]

The Comment, however, does not define the term "special security measures," except indirectly by using language similar to the one used in ABA Formal Opinion 99-413 on encryption of confidential information. [136] Instead, the Comment can provide examples of "special security measures," such as the use of encryption to protect sensitive client information and attorney-client communications. [137]

Some Cautionary Reflections, 2009 J. Prof. Law. 1, 4-7 (2009) (arguing that future reform to the regulation of lawyers may require abandoning the state-based approach); Eli Wald, Federalizing Legal Ethics, Nationalizing Law Practice and the Future of the American Legal Profession in a Global Age, *48 San Diego L. Rev. 489 (2011);* Fred C. Zacharias, Federalizing Legal Ethics, *73 Tex. L. Rev. 335 (1994);* see also Ted Schneyer, Professional Discipline in 2050: A Look Back, *60 Fordham L. Rev. 125, 127 (1991)* (predicting the adoption of a "Federal Code of Lawyering"). Of course, states may act independent of the ongoing federalization of legal ethics and regulate the practice of law within their jurisdictions. See, e.g., *Cal. Bus. & Prof. Code § 6000* (West 2016).

[133] See Peter A. Joy, Making Ethics Opinions Meaningful: Toward More Effective Regulation of Lawyers' Conduct, *15 Geo. J. Legal Ethics 313, 317-19 (2002).*

[134] Model Rules of Prof'l Conduct r. 1.6 cmt. 18 (Am. Bar Ass'n 2013).

[135] Id. r. 1.6 cmt. 19 (emphasis added).

[136] See ABA Comm. on Ethics & Prof'l Responsibility, supra note 84.

[137] See proposed Comment U, Appendix A.

Next, the Comment may explicitly state that a lawyer who fails to take the most basic security precautions violates Rule 1.6(c), even if the client's information was accessed by a third party criminally. In other words, the Comment should state that the criminal conduct of third parties does not constitute a safe harbor to lawyers who fail to make "reasonable efforts" to protect the information. Historically, the Rules made attorneys liable for their own conduct, for example, inadvertently disclosing **[*533]** confidential client information, but not for the criminal actions of third parties. "This view," explains Alan Ezekiel, "that attorneys are not responsible for violations of client privacy that flow from criminal misconduct by third parties may have been informed by the evolution of legal standards regarding the use of mobile phones." [138] Whereas early ethics opinions in the 1990s suggested that attorneys might violate rules of professional conduct by discussing private client information on mobile phones because outsiders could overhear the conversations, later opinions reflected the view that "the Electronic Communications Privacy Act (which criminalized interception of wireless telephone conversations) created a reasonable expectation of privacy on a mobile phone, and thus the attorney could discuss client matters on a mobile phone without violating any ethical standards." [139] Importantly, "the fact that an outsider might be able to overhear the conversation was irrelevant," adds Ezekiel, "because the outsider would thereby be committing a felony." [140]

Similarly, because "[a] hacker would be committing a felonious violation of the Computer Fraud and Abuse Act by accessing client records without authorization," [141] Comment 19's statement that the duty to protect client information "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy" [142] can be read to suggest that an attorney who fails to prevent unauthorized criminal access to client information is not acting unreasonably. "But," asked Ezekiel compellingly, "should the fact that hacking is illegal excuse an attorney who fails to take even the most basic security precautions in an era of widespread data theft?" [143]

Of course, that a third party commits a crime to access client information is relevant in terms of determining the consequences for the client. For example, because the attorney-client privilege belongs to the client, only the behavior of the client - holder of the privilege - or the client's lawyer-agent can waive it. Therefore, in most jurisdictions, intercepted communications are still privileged, meaning that client information stolen from the lawyer would nonetheless continue to be privileged. [144] Such attempts to mitigate the consequences of information theft for **[*534]** victim-clients ought not, however, negate the misconduct of an attorney who fails to utilize basic cybersecurity measures to protect client information.

Thus, in addition to offering examples of "special security measures" and the circumstances which warrant them, the Comment to Rule 1.6 must clearly state that a third party's criminal activity accessing clients' information does not negate the responsibility of a lawyer who fails to take reasonable cybersecurity measures on behalf of clients. Comment V to Rule 1.6 may accordingly add that:

the unauthorized access to information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. However, an unauthorized access to information relating to the representation of a client may constitute a violation of paragraph (c) if the lawyer has not made reasonable efforts to prevent the access, even if a third party accessed the information unlawfully. [145]

---

[138] Ezekiel, supra note 13, at 659.

[139] Id.

[140] Id. at 659-60.

[141] Id.

[142] Model Rules of Prof'l Conduct r. 1.6 cmt. 19 (Am. Bar Ass'n 2013).

[143] Ezekiel, supra note 13, at 660.

[144] Hughes, supra note 26, at 417-18.

[145] For a redline of the proposed revisions to the Rules, see Appendix A.

4. Disclosure of Cyberattacks and Data Theft to Clients

The Rules do not impose a general duty on lawyers to advise clients when their information has been compromised in a cyberattack, let alone that the law firm was or is under attack. [146] Rule 1.4(a)(3) only requires lawyers to "keep the client reasonably informed about the status of the matter," which Comment 3 explains means advising clients regarding "significant developments affecting the … substance of the representation." [147] Yet, as we have seen, because often the identity of the attacker, the nature of the information compromised, and the extent of the damage to the client are unknown, a lawyer may not be in a position to conclude that the cyberattack or data theft constitute "a significant development" as opposed to a mere development, and so Rule 1.4(a)(3) is not triggered. Similarly, the inherent uncertainty often surrounding cyberattacks means that Rule 1.4(b)'s admonition for lawyers to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation" [148] may not be triggered because the impact on the matter at hand may be less than clear to the lawyer.

[*535] This prevailing interpretation of Rule 1.4 finds some support in the recent rule amendments regarding cybersecurity. Comment 18 on Rule 1.6 states in relevant part that:

whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. [149]

Read narrowly, the Comment merely states the obvious, namely, that the Rules never, and do not in the case of cybersecurity, purport to construe "other law" such as state and federal laws that may or may not impose additional duties on lawyers. Yet the Comment may also imply or may be read by some lawyers to suggest that notification requirements to clients upon the loss or unauthorized access to their information are beyond the scope of the Rules.

The better interpretation of Rule 1.4, however, is that it does impose an affirmative duty on lawyers to notify clients when their confidential information has been compromised, even when the consequences and impact of the attacks on clients' information fall short of the "significant development" threshold of Rule 1.4(a)(3) or the duty to explain a matter and the means by which it is to be pursued to a client per 1.4(b). To see why imposing a disclosure duty is warranted, recall that Rule 1.4(a)(3), as construed by Comment 3, does impose a duty on lawyers to advise clients regarding a significant development affecting the representation. The Rule assumes that in most circumstance a lawyer would be able to determine whether a particular development is either significant (and therefore triggers 1.4(a)(3)) or less than significant (such that 1.4(a)(3) is not triggered). Cyberattacks, however, are an example of a circumstance possibly not anticipated by the Rules - one in which inherent uncertainty prevents a lawyer from reasonably concluding whether a development affecting the matter is significant or not. In such a case, lawyers as agents and fiduciaries of clients must err on the side of caution and advise their principals-clients of the development. [150] That is, in the face **[*536]** of inherent uncertainty regarding the impact of cyberattacks and whether client information has been compromised, a question arises as to whether clients should know more or less

---

[146] See supra Section III.A.

[147] Model Rules of Prof'l Conduct r. 1.4(a)(3).

[148] Id. r. 1.4(b).

[149] Id. r. 1.6 cmt. 18 (emphasis added).

[150] Elsewhere, I argue that Rule 1.4 should be revised and/or interpreted to mean that lawyers must advise clients regarding all material developments regarding the representation. See Eli Wald, Taking Attorney-Client Communications (and Therefore Clients) Seriously, *42 U.S.F. L. Rev. 747, 789-91 (2008).* Inherent uncertainty regarding cyberattacks may leave lawyers unable to determine whether an attack constitutes a material development affecting the representation. Taking attorney-client communications, and therefore clients, seriously dictates that when faced with such inherent uncertainty, lawyers must err on the side of disclosing more rather than less information relating to the representation to clients. *Id. at 748-50.*

about the development. Because clients are the principals in the attorney-client relationship and lawyers are mere agents-fiduciaries, it appears that in the face of inherent uncertainty, lawyers must err on the side of more, rather than less, disclosure to clients. This interpretation is especially compelling in the context of cyberattacks, in which clients, as opposed to lawyers, would often be in the best position to assess the impact of and respond to cyberattacks. [151]

Acknowledging that in general, lawyers must tell clients more about compromised client information requires detailing when lawyers must communicate with clients - identifying the specific triggering event for disclosure - and how they ought to go about discussing cyberattacks and their consequences with clients. In this regard, the Rules may learn from existing states' personal information data breach notification statutes. [152] For example, *California Civil Code section 1798.82(a)* states that:

(a) A person or business … that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a [person] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay … . [153]

California's statutory notification provision is noteworthy in at least two ways. First, while it imposes a mandatory duty to notify customers, [154] the duty is triggered only when the protected information was or is reasonably believed to have been compromised. [155] The provision, to be clear, does not impose a notification duty when a cybersecurity system storing protected information is under a cyberattack, presumably because such a trigger would reveal little to customers if the system was able to thwart the attack. Rather, notification is mandated either when protected information was compromised, or, in the face of some uncertainty, when it is reasonable to assume that the protected information has been compromised. Second, the statute only requires notification when a person's "unencrypted personal **[*537]** information was, or is reasonably believed to have been, acquired by an unauthorized person." [156] That is, because the statute only requires notification when unencrypted information was or is reasonably believed to have been compromised, arguably encryption of the information provides a practical safe harbor and negates the need to disclose a breach.

The statutory experience thus suggests two models the Rules can follow. Akin to California's notification apparatus, a modest revision to the Rules can require disclosure to clients only when a client's confidential information has been or is reasonably believed to have been compromised, and only if the confidential information was not reasonably protected, such that if a lawyer reasonably protects the information (via encryption or otherwise) no disclosure to clients would be mandated. For example, the Rules may be amended to state that:

A lawyer who stores (or employs a third party provider to store) information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose unreasonably protected confidential information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.

---

[151] See Goldberg, supra note 25, at 540-41.

[152] McNerney & Papadopoulos, supra note 12, at 1254-56.

[153] *Cal. Civ. Code § 1798.82(a)* (West 2016).

[154] Id. ("shall disclose a breach of the security of the system").

[155] Id. ("whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person").

[156] Id. (emphasis added).

Such a disclosure provision would naturally follow and complement the above proposals requiring all lawyers to adopt cybersecurity plans for all their clients and to make reasonable efforts to protect clients' confidential information. Lawyers who take these two steps would, practically speaking, have no duty to report to clients when their information has been or is reasonably believed to have been compromised because they would be covered by a safe harbor of reasonableness.

In the alternative, the Rules may adopt the triggering event of the personal information notification statutes - information that was or is reasonably believed to have been compromised - without excusing disclosure to clients even when the lawyer did make reasonable efforts to protect the information. Comment W to Rule 1.4 should read:

A lawyer who stores (or employs a third party provider to store) information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose confidential information was, or is reasonably believed to have been, acquired by **[*538]** an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay. [157]

The latter approach appears to be warranted in the context of the attorney-client relationship. When a client's confidential information was or is reasonably believed to have been compromised, clients must be advised, even if the lawyer did make reasonable efforts to protect the information. One might argue that when a lawyer has made reasonable efforts to protect the information, imposing a mandatory duty on lawyers to advise clients that their information was, or is, reasonably believed to have been compromised is likely to be ineffective - burdening the client with irrelevant information, with possible distinct adverse consequences, such as chilling or eroding the attorney-client relationship. Put differently, would not mandating adoption of cybersecurity plans and spelling out reasonable efforts be enough? If these provisions end up ensuring reasonable conduct by lawyers, why force disclosure and risk clients developing "notice fatigue"? Would not clients be content with lawyers' adoption of reasonable efforts? If nothing else could have been reasonably done by lawyers, why tire the clients with additional disclosures?

These objections, however, must be rejected for three related reasons. First, they smack of lawyers' self-interest at the expense of clients, the very concern about and criticism of the Rules to which lawyers ought to be sensitive. [158] No doubt, reporting to a client that the client's confidential information was or is reasonably believed to have been compromised is likely to be awkward to the lawyer, [159] but that is not in and of itself a legitimate ground a lawyer should be able to invoke to avoid disclosing information to the client.

Second, recall that this Article advocates a revision to the Comment to Rule 1.6, pursuant to which "a lawyer must adopt reasonable procedures … appropriate for the size and type of firm and practice, to protect a client's information," including reasonable cybersecurity procedures. [160] With such a cybersecurity plan in place, a lawyer's communication to a client regarding a breach and compromised information following a cyberattack is **[*539]** unlikely to chill the attorney-client relationship, because a lawyer would be able to cheaply and effectively explain to the client the reasonable efforts the law firm made to protect the client's information, and the inherent uncertainty surrounding the cyberattack, notwithstanding the reasonable security measures undertaken. Indeed, it is the current state of technology that prevents lawyers (and others) from stopping all cyberattacks and reasonable clients should be able to understand and accept a lawyer's reasonable conduct in the face of technological limitations and uncertainty.

---

[157] For a redline of the proposed revisions to the Rules, see Appendix A, proposed Comment W to Rule 1.4.

[158] See supra notes 45-46 and accompanying text.

[159] Recall that if a cyberattack has in fact resulted in disclosure of a client's material confidential information, then even a traditional reading of 1.4(a)(3) and 1.4(b) will mandate disclosure to the client. See Model Rules of Prof'l Conduct r. 1.4(a)(3), 1.4(b) (Am. Bar Ass'n 2013).

[160] See supra note 123 and accompanying text.

Finally, any interpretation second-guessing disclosing information to clients when confidential information was or is reasonably believed to have been compromised on the ground that clients may not understand it or will be fatigued smacks of lawyers' paternalism vis-a-vis clients, inappropriate in the attorney-client relationship. [161] As I explain elsewhere, "for lawyers to assume that clients are unable to comprehend and appreciate the consequences and meaning of complex … information, even when offered a detailed explanation … would constitute unacceptable paternalistic withholding of material information." [162] The U.S. Supreme Court, in its landmark decision, Basic, Inc. v. Levinson, [163] construed the term "material" in securities law. It held that to address inherent uncertainty by not disclosing material information to clients amounts to assuming that clients are

nitwits, unable to appreciate - even when told - that [cybersecurity measures] are risky propositions … . Disclosure, and not paternalistic withholding of accurate information, is the [desirable] policy … . The role of the materiality requirement is not to "attribute to [clients] a child-like simplicity, an inability to grasp the probabilistic significance of [cybersecurity measures]' … but to filter out essentially useless information that a reasonable [client] would not consider significant, even as part of a larger "mix' of factors to consider in making his … decision [164]

regarding the attorney-client relationship.

Moreover, fatigue assumes that clients would know and may not care or become indifferent about security breaches. Yet the assumption seems inapplicable here. Currently, clients do not usually learn about, and are unlikely to be indifferent about breaches regarding their confidential information. For the same reason, mandating disclosure to clients only when the unauthorized access of confidential information is likely to have a **[*540]** prejudicial impact on their representation would not suffice. Just as the inherent uncertainty surrounding cyberattacks often precludes lawyers from concluding that a breach of confidential information constitutes a "significant development" mandating disclosure to clients, the same uncertainty will likely prevent lawyers from concluding that a breach has a prejudicial impact on clients' representation. Because a reasonable client would like to know when her confidential information was, or is, reasonably believed to have been accessed by an unauthorized party, a lawyer must disclose accordingly.

Mandating disclosure to clients when confidential information was, or is, reasonably believed to have been compromised has one additional important benefit. Disclosure would, in turn, enable clients to sanction lawyers who fail to put in place "reasonable efforts" to protect their confidential information and reward lawyers who do make reasonable efforts to protect confidential information. Put differently, the adoption of a rule of professional conduct mandating disclosure of cybersecurity information to clients would allow clients to exercise market controls over lawyers, further addressing the underregulation of lawyers' cybersecurity conduct. Finally, even if lawyers do make reasonable efforts to protect confidential information, a disclosure duty would result in more conversations with clients about cybersecurity, allowing clients to participate on an informed basis regarding the cyber means by which their objectives are to be pursued.

Conclusion

The inherent uncertainty often surrounding cyberattacks on law firms - who specifically perpetrated the attack, what information was stolen or compromised, and what damage, if any, did a client suffer as a result of the attack - renders liability rules, such as malpractice suits, and market controls, such as being fired by a client, ineffective in regulating lawyers' cybersecurity conduct. The Rules thus have an opportunity to play a meaningful role in informing and guiding the conduct of underregulated lawyers, by requiring lawyers to adopt and implement cybersecurity plans for all clients, defining the meaning of "reasonable efforts" necessary to prevent the unauthorized disclosure

---

[161] Model Rules of Prof'l Conduct r. 1.2(a).

[162] Wald, supra note 150, at 795.

[163] *Basic Inc. v. Levinson, 485 U.S. 224 (1988).*

[164] *Id. at 234;* see also Wald, supra note 150, at 795-96.

or access to information relating to the representation of a client, and by mandating disclosure to clients when their confidential information was, or is, reasonably believed to have been accessed by an unauthorized party.

[*541]

Appendix A: Proposed Revisions to the Rules

Proposed revisions to the Rules are italicized.

Comment on Rule 1.6

Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

[X] To competently safeguard information relating to the representation of a client against unauthorized access by third parties, a lawyer must adopt reasonable procedures, including reasonable cybersecurity measures, appropriate for the size and type of firm and practice, to protect a client's confidential information. Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule.

The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

[Y] Reasonable efforts to prevent the inadvertent or unauthorized disclosure of information relating to the representation of a client would normally include robust strategies for identifying, prioritizing, and securing valuable information; periodical inspection of the firm's information storage system for signs of cyberattacks and data theft; the use of basic cybersecurity measures, including the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords updated from time to time, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents; and the adoption of cybersecurity training protocols for firm lawyers and staff. See Rule 5.1 and 5.3.

Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing **[*542]** additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

[Z] Whether a lawyer may be required to take additional special security measures to safeguard a client's information, above and beyond basic cybersecurity measures, depends on the circumstances. For example, a lawyer may be required to take special security measures to protect sensitive information related to the representation of a client.

A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules, but see Rule 1.4, Comment [U]. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended

recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.

[U] Special security measures may include encryption of attorney-client communications or password-protecting information relating to the representation of a client on the lawyer's or law firm's information storage system.

Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws **[*543]** that govern data privacy, is beyond the scope of these Rules, but see Rule 1.4, Comment [3].

[V] The unauthorized access to information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. However, an unauthorized access to information relating to the representation of a client may constitute a violation of paragraph (c) if the lawyer has not made reasonable efforts to prevent the access, even if a third party accessed the information unlawfully.

Comment on Rule 1.4

Communicating with Client

[3] Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations - depending on both the importance of the action under consideration and the feasibility of consulting with the client - this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[W] A lawyer who stores (or employs a third party provider to store) information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose confidential information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.

End of Document

The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INTERNATIONAL INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 21

UNITED STATES

Alan Charles Raul, Tasha D Manoranjan and Vivek Mohan[1]

I OVERVIEW

Though not universally acknowledged, the United States' commercial privacy regime is arguably the oldest, most robust, well developed and effective in the world. The United States' privacy system has a relatively flexible and non-prescriptive nature, relying more on *post hoc* government enforcement and private litigation, and on the corresponding deterrent value of such enforcement and litigation, than on detailed prohibitions and rules. With certain notable exceptions, the US system does not apply a 'precautionary principle' to protect privacy, but rather, allows injured parties (and government agencies) to bring legal action to recover damages for, or enjoin, 'unfair or deceptive' business practices. However, US federal law does impose affirmative prohibitions and restrictions in certain commercial sectors, such as those involving financial and medical data, and electronic communications, as well as with respect to children's privacy, background investigations and 'consumer reports' for credit or employment purposes, and certain other specific areas. State laws add numerous additional privacy requirements.

Legal protection of privacy in civil society has been recognised in the US common law since 1890 when the article 'The Right to Privacy' was published in the *Harvard Law Review* by Professors Samuel D Warren and Louis D Brandeis. Moreover, from its conception by Warren and Brandeis, the US system for protecting privacy in the commercial realm has been focused on addressing technological innovation. The Harvard

1 Alan Charles Raul is a partner and Tasha D Manoranjan and Vivek Mohan are associates at Sidley Austin LLP. Passages of this chapter were originally published in 'Privacy and data protection in the United States', *The Debate on privacy and security over the network: Regulation and markets, 2012*, Fundación Telefónica; and Raul and Mohan, 'The Strength of the U.S. Commercial Privacy Regime', 31 March 2014, a memorandum to the Big Data Study Group, US Office of Science and Technology Policy.

professors astutely noted that '[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual […] the right "to be let alone"'. In 1974, Congress enacted the federal Privacy Act, regulating government databases, and found that 'the right to privacy is a personal and fundamental right protected by the Constitution of the United States'. It is generally acknowledged that the US Privacy Act represented the first official embodiment of the fair information principles and practices that have been incorporated in many other data protection regimes, including the European Union's 1995 Data Protection Directive.

The US has also led the way for the world not only on establishing model legal data protection standards in the 1974 Privacy Act, but also in terms of imposing affirmative data breach notification and information security requirements on private entities that collect or process personal data from consumers, employees and other individuals. The state of California was the path breaker on data security and data breach notification by first requiring in 2003 that companies notify individuals whose personal information was compromised or improperly acquired. Since then, approximately 47 states, the District of Columbia and other US jurisdictions, and the federal banking, health-care and communications agencies have also required companies to provide mandatory data breach notification to affected individuals, and imposed affirmative administrative, technical and physical safeguards to protect the security of sensitive personal information. Dozens of other medical and financial privacy laws also exist in various states. There is, however, no single omnibus federal privacy law in the US. Moreover, there is no designated central data protection authority in the US, though the Federal Trade Commission (FTC) has essentially assumed that role for consumer privacy. The FTC is independent of the President, and is not obliged (though it is encouraged) to respect the Administration's perspective on the proper balance between costs and benefits with respect to protecting data privacy.

As in the EU and elsewhere, privacy and data protection are balanced in the US in accordance with other rights and interests that societies need to prosper and flourish, namely, economic growth and efficiency, technological innovation, property and free speech rights and, of course, the values of promoting human dignity and personal autonomy. The most significant factor in counterbalancing privacy protections in the US, perhaps, is the right to freedom of expression guaranteed by the First Amendment. Preserving free speech rights for everyone certainly entails complications for a 'right to be forgotten' since one person's desire for oblivion may run counter to another's sense of nostalgia (or some other desire to memorialise the past for good or ill).

The First Amendment has also been interpreted to protect the people's right to know information of public concern or interest, even if it trenches to some extent on individual privacy. Companies have also been deemed to have a First Amendment right to communicate relatively freely with their customers by exchanging information in both directions (subject to the information being truthful, not misleading, and otherwise not the subject of an unfair or deceptive business practice).

The dynamic and robust system of privacy governance in the United States marshals the combined focus and enforcement muscle of the US Federal Trade Commission, state attorneys general, the Federal Communications Commission, the Securities and Exchange Commission, the Consumer Financial Protection Bureau (and other financial and banking regulators), the Department of Health and Human Services,

the Department of Education, the judicial system, and last – but certainly not least – the highly motivated and aggressive US plaintiffs' bar. Taken together, this enforcement ecosystem has proven to be nimble, flexible, and effective in adapting to rapidly changing technological developments and practices, responding to evolving consumer and citizen expectations, and serving as a meaningful agent of deterrence and accountability. Indeed, the US enforcement and litigation-based approach appears to be particularly well suited to deal with 'recent inventions and business methods' – namely, new technologies and modes of commerce – that pose ever changing opportunities and unpredictable privacy challenges.

II THE YEAR IN REVIEW

As with nearly other area of recent legislative activity in Washington, Congress has not been able to act on privacy, consumer data security, data breach notification or cybersecurity legislation. While the Administration of President Obama has called upon Congress to enact a 'Consumer Privacy Bill of Rights' and legislation to help protect cybersecurity for 'critical infrastructure', partisan gridlock, as well as concern about over-regulating the private sector, has stalled action. The congressional stalemate was considerably shaken up, however, when former National Security Agency (NSA) contractor Edward Snowden leaked information regarding US government surveillance programmes to *The Guardian* and *The Washington Post* in the summer of 2013. This sparked a media frenzy around various NSA surveillance programmes. Some of the allegations concerned unauthorised surveillance of US citizens or foreign intelligence targets within the United States, while others suggested widespread surveillance outside the US.

As a result of these disclosures, foreign governments, including within the European Union, expressed concern regarding the breadth of NSA surveillance outside the United States. For example, the EU Article 29 Working Party sent a letter to EU Justice Commissioner Viviane Reding suggesting a possible investigation of violations by the US of the EU's data protection rules.[2]

The media and political firestorm surrounding the Snowden disclosures has led the executive branch to introduce proposals regarding NSA and commercial data collection processes. In addition to its proposals for reforms of the government's bulk metadata surveillance, the White House has also issued reports and recommendations for data collection in the private big data sector. Following closely on this, on 29 May the FTC issued a much anticipated report on big data that heavily criticised the lack of transparency in the data brokering industry, offered recommendations for consumer control of information and advocated for broad legislation that would not only create obligations for analytics companies, but also for retailers that may provide them with information. Significantly, however, the report does not suggest that any current data broker practices are illegal under existing law.

2 See Jacob Kohnstamm, Chairman of EU Article 29 Working Party, letter to Viviane Reding (13 August 2013), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf.

Cybersecurity remains a hot topic, although expectations for congressional action remain uncertain. Legislative action in the states continues, with Kentucky becoming the 47th state to have passed data breach notification legislation. Several states have also amended existing laws to expand breach obligations.

FTC actions

The FTC announced on 21January 2014 that it had entered into no-fault consent orders with 12 companies that allegedly claimed they were in compliance with the US–EU and US–Switzerland Safe Harbor programmes when in fact their certifications had lapsed. The agreement covers several large businesses, including three NFL football teams and Level 3 Communications LLC, one of the largest internet service providers in the world. The Safe Harbor programme requires companies to annually re-certify their compliance with the Safe Harbor framework. The FTC charged that by including statements in their privacy policies or posting certification notices that falsely indicated current compliance, these companies violated Section 5 of the FTC Act, which prohibits deceptive business practices. The settlements included no allegations of substantive violations of the Safe Harbor framework.

The FTC also brought an action against Jerk.com in April 2014 for allegedly deceptive practices. Jerk.com allegedly obtained the personal information of Facebook users and created profiles of people labelled 'Jerk' and 'not a Jerk.' Jerk.com then offered consumers the opportunity to pay US$30 to revise their profiles. The FTC alleged that such practices were misleading because the website stated that other Jerk.com users had created such profiles whereas most of the information had been pulled directly from Facebook by the operators of Jerk.com. In total, the FTC alleges that Jerk.com collected profiles on more than 73 million people, much of which had been designated as private by the users on Facebook. The FTC sought an order prohibiting such practices, including the use of personal information that is improperly obtained.

Interestingly, this case indicates that unauthorised scraping may be challenged not only by the website from which data is collected, but by regulators. The FTC's charges specifically alleged that the company 'harvested personal information from Facebook', and in the FTC's press release, they specifically noted that they were 'seeking an order barring the defendants' deceptive practices, prohibiting them from using the personal information they improperly obtained, and requiring them to delete the information'. The complaint also cited the restrictive authorisation terms of the social media site's platform agreement.

The FTC settled charges with Snapchat in May 2014 over the company's alleged deceptive privacy and confidentiality marketing promises. According to the complaint, the company, which currently transmits over 700 million messages back and forth each day, marketed its messaging services by telling users that the messages 'disappear forever', while in reality, the messages can be saved in several ways. In addition, the FTC alleged that Snapchat transmitted users' location data and transmitted sensitive information like address book contacts although the company told consumers it did not collect such information. The settlement prohibits Snapchat from misrepresenting how it maintains the privacy and confidentiality of user information and the company will also have to start a privacy programme that will be independently monitored for 20 years. If the company does not comply, it could face fines. The company has said it has resolved most

of these concerns over the last year and has improved the wording of its privacy policy, app description, and in-app just-in-time notifications.

In July 2012, following a significant data breach affecting hotel guest information, the FTC sued Wyndham Worldwide Corporation for failure to maintain reasonable and appropriate security measures. Wyndham, a hotel chain and licensing company that suffered at least three data breaches between 2008 and 2010, challenged the FTC's authority to bring an enforcement action under the unfairness prong of their Section 5 authority. In April 2014, a federal district judge in New Jersey rejected Wyndham's motion to dismiss, holding that the FTC could use its general, and flexible, 'unfairness' authority to enforce against companies that cause consumer and business harm because of weak data security systems. The court also ruled it was not necessary for Congress to provide express data security authority, or for the FTC to publish regulations specifying in detail what security practices would be deemed reasonable and appropriate. The case is currently on appeal.

The Puerto Rico Health Administration issued an unprecedented US$6.8 million fine in February 2014 against Triple-S Salud Inc, a Puerto Rican licensee of Blue Cross Blue Shield of Puerto Rico that handles managed care for Medicare enrollees. Triple-S admitted to accidentally sending out pamphlets with visible claim numbers to 70,000 Medicare Advantage customers.

II REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The US has specific privacy laws for the types of citizen and consumer data that are most sensitive and at risk: financial, insurance and medical information; information about children and students; telephone, internet and other electronic communications and records; credit and consumer reports and background investigations, at the federal level, and a further extensive array of specific privacy laws at the state level. Moreover, the US is the unquestioned world leader in mandating information security and data breach notification, without which information privacy is not possible. If one of the sector-specific federal or state laws does not cover a particular category of data or information practice, then the Federal Trade Commission Act, and each state's 'little FTC Act' analogue, comes in to play. Those general consumer protection statutes broadly, flexibly and comprehensively proscribe (and authorise tough enforcement against) 'unfair or deceptive' acts or practices. The FTC is the *de facto* privacy regulator in the US. It should also be noted that state attorneys general, and private plaintiffs, can also enforce privacy standards under analogous 'unfair and deceptive acts and practices' standards in state law. Additionally, information privacy is further protected by a network of common law torts, including invasion of privacy, public disclosure of private facts, 'false light,' appropriation or infringement of the right of publicity or personal likeness, and of course, remedies against general misappropriation or negligence. In short, there are no substantial lacunae in the regulation of commercial data privacy in the US. In taking both a general (unfair or deceptive) and sectoral approach to commercial privacy governance, the United States has empowered government agencies to oversee data privacy where the categories and uses of data could injure individuals.

FTC Act

Section 5 of the Federal Trade Commission Act (FTC Act) prohibits 'unfair or deceptive acts or practices in or affecting commerce'. While the FTC Act does not expressly address privacy or information security, the FTC applies Section 5 to information privacy, data security, online advertising, behavioural tracking, and other data intensive, commercial activities. The FTC has brought successful enforcement actions under Section 5 against companies that failed to adequately disclose their data collection practices, failed to abide by the promises made in their privacy policies, failed to comply with their security commitments, or failed to provide a 'fair' level of security for consumer information.

Under Section 5, an act or practice is deceptive if: (1) there is a representation or omission of information likely to mislead a consumer acting reasonably under the circumstances; and (2) the representation or omission is 'material' – defined as an act or practice 'likely to affect the consumer's conduct or decision with regard to a product or service'. An act or practice is 'unfair' under Section 5 if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and lacks countervailing benefits to consumers or competition.

The FTC takes the position that companies must disclose their privacy practices adequately, and that in certain circumstances, this may require particularly timely, clear and prominent notice, especially for novel, unexpected or sensitive uses. The FTC brought an enforcement action in 2009 against Sears for allegedly failing to adequately disclose the extent to which it collected personal information by tracking the online browsing of consumers who downloaded certain software. The consumer information allegedly collected included 'nearly all of the Internet behavior that occurs on […] computers'. The FTC required Sears to prominently disclose any data practices that would have significant unexpected implications in a separate screen outside of any user agreement, privacy policy or terms of use.

Section 5 is also generally understood to prohibit a company from using previously collected personal data in ways that are materially different, and less protective, than what it initially disclosed to the data subject, without first obtaining the individual's additional consent.

The FTC staff has also issued extensive guidance on online behavioural advertising, emphasising four principles to protect consumer privacy interests: (1) transparency and control, giving meaningful disclosure to consumers, and offering consumers choice about information collection; (2) maintaining data security, and limiting data retention; (3) express consent before using information in a manner that is materially different from the privacy policy in place when the data was collected; and (4) express consent before using sensitive data for behavioural advertising. The FTC's report does not, however, require opt-in consent for the use of non-sensitive information in behavioural advertising.

Fair information practice principles

The innovative American privacy doctrine elaborated theories for tort and injunctive remedies for invasions of privacy (including compensation for mental suffering). The Warren–Brandeis right to privacy, along with the right to be let alone, was followed in 1973 by the first affirmative government undertaking to protect privacy in the computer age. The new philosophy was expressed in The Secretary's Advisory Committee on

Automated Personal Data Systems, published by the US Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services). This report developed the principles for 'fair information practices' that were subsequently adopted by the US in the 1974 Privacy Act, and ultimately, by the European Union in 1995 in its Data Protection Directive. The fair information practice principles established in the US in 1973–74 remain largely operative around the world today in regimes and societies that respect information privacy rights of individuals. The fundamental US HEW/Privacy Act principles were:

a there must be no personal data record-keeping systems whose very existence is secret;

b there must be a way for an individual to find out what information about him or her is in a record and how it is used;

c there must be a way for an individual to prevent information about him or her obtained for one purpose from being used or made available for other purposes without his or her consent;

d there must be a way for an individual to correct or amend a record of identifiable information about him or her; and

e any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Classification of data

The definitions of personal data and sensitive personal data vary by regulation. The FTC considers information that can reasonably be used to contact or distinguish an individual (including IP addresses) to constitute personal data (at least in the context of children's privacy). Generally, sensitive data includes personal health data, credit reports, personal information collected online from children under 13, precise location data, and information that can be used for identity theft or fraud.

Federal laws

Congress has passed laws protecting personal information in the most sensitive areas of consumer life, including health and financial information, information about children, and credit information. Various federal agencies are tasked with rule making, oversight, and enforcement of these legislative directives.

The scope of these laws and the agencies that are tasked with enforcing them is formidable. Laws such as Children's Online Privacy Protection Act of 1998, the Health Insurance Portability and Accountability Act of 1996, the Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act or GLBA), the Fair Credit Reporting Act, the Electronic Communications Privacy Act, the Communications Act (regarding consumer proprietary network information) and the Telephone Consumer Protection Act of 1991, to name just a few, prescribe specific statutory standards to protect the most sensitive consumer data.

State laws

In addition to the concurrent authority that state attorneys general share for enforcement of certain federal privacy laws, state legislatures have been especially active on privacy

issues that states view worthy of targeted legislation. In the areas of online privacy and data security alone, state legislatures have passed laws covering a broad array of privacy-related issues,[3] cyberstalking,[4] data disposal,[5] privacy policies, security breach notification,[6] employer access to employee social media accounts,[7] unsolicited commercial communications[8] and electronic solicitation of children,[9] to name but a few.

California is viewed as a leading legislator in the privacy arena, and its large population and high-tech sector means that the requirements of California law receive particular attention and often have *de facto* application to businesses operating across the United States.[10] The combined legislative and enforcement authority of federal and state governments ensures that the policy leadership articulated at the federal level – like the White House's 2012 Privacy Report – can be implemented effectively in practice.

Co-regulation and industry self-regulation

To address concerns about privacy practices in various industries, industry stakeholders have worked with government, academics, and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively-developed accountability programmes establish expected practices for use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. This approach has had notable success, such as the development of the 'About Advertising' icon by the Digital Advertising Alliance and the opt-out for cookies set forth by the Network Advertising Initiative.[11] Companies that assert their compliance with, or membership in, these self-regulatory initiatives must comply with these voluntary standards or risk being deemed to have engaged in a deceptive practice. The same is true for companies that publish privacy policies – a company's failure to comply with its own privacy policy is a quintessentially deceptive practice. It should also be noted

3 See www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

4 See www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx.

5 See www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

6 See www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

7 See www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

8 See www.ncsl.org/research/telecommunications-and-information-technology/unsolicited-commercial-communication-laws.aspx.

9 See www.ncsl.org/research/telecommunications-and-information-technology/electronic-solicitation-or-luring-of-children-sta.aspx.

10 See https://oag.ca.gov/privacy/privacy-laws.

11 See www.aboutads.info/; www.networkadvertising.org/choices/?partnerId=1//.

that various laws require publication or provision of privacy policies, including for example, the GLBA (financial data), HIPAA (health data) and California law (websites collecting personal information). In addition, voluntary membership or certification in various self-regulatory initiatives also requires posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming detrimental reliance on such policies.

ii General obligations for data handlers

There is no requirement to register databases in the United States. Depending on the context, data handlers may be required to provide data subjects with pre-collection notice, and the opportunity to opt out for use and disclosure of regulated personal information. Information that is considered sensitive personal information, such as health information, may involve opt-in rules. The FTC considers it a deceptive trade practice if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was obtained.

iii Technological innovation and privacy law

Electronic marketing is extensively regulated in the US through a myriad of laws. The CAN-SPAM Act is a federal law governing commercial e-mail messages. Generally, a company is permitted to send commercial emails to anyone under CAN-SPAM, provided these conditions are met: the recipient has not opted out of receiving such e-mails from the company, the e-mail identifies the sender and the sender's contact information, and the e-mail has instructions on how to easily and at no cost opt out of future commercial e-mails from the company.

Generally, express, written consent is required for companies to send marketing text messages. Marketing texts are a significant class action risk area.

There is no specific federal law that regulates the use of cookies and other similar online tracking tools. However, the use of tracking mechanisms should be carefully and fully disclosed in a company's website privacy policy. Additionally, it is a best practice for websites that allow online behavioural advertising to participate in the Digital Advertising Alliance code of conduct, which enables users to easily opt out of being tracked for these purposes. California law imposes further requirements on online tracking. California requires companies that track personally identifiable information over time and multiple websites to disclose how the company responds to 'do-not-track' signals and whether users can opt out of such tracking.

Location tracking is currently a subject of interest and debate. Federal Communications Commission regulations govern the collection and disclosure of certain location tracking by the telecommunications providers (generally speaking, telephone carriers). Additionally, the FTC and California have issued best-practice recommendations for mobile apps and mobile app platforms.

The Department of Commerce's National Telecommunications and Information Administration led a multi-stakeholder negotiation to develop a code of conduct for mobile app privacy. The draft code of conduct issued July 2013 is available online.[12]

iv Specific regulatory areas

The US system of privacy is composed of laws and regulations that focus on particular industries (financial services, health care, communications), particular activities (i.e., collecting information about children online) and particular types of data.

Federal legislation

Financial privacy

For financial privacy, the federal banking agencies and the FTC were, until recently, primarily responsible for enforcing consumer privacy under the GLBA, which applies to financial institutions. Following the recent Dodd-Frank legislation, such laws will be primarily (but not exclusively) enforced by the new Consumer Financial Protection Bureau, which has significant, independent regulatory and enforcement powers. The FTC, however, will remain primarily responsible for administering the Fair Credit Reporting Act, along with the general unfair and deceptive acts and practices standards under the FTC Act and the Children's Online Privacy Protection Act 1998 (COPPA), which imposes affirmative privacy and security duties on entities that collect personal information from children under 13 years of age.

The Financial Services Modernization Act of 1999 or GLBA addresses financial data privacy and security by establishing standards for safeguarding customers' 'non-public personal information' – or personally identifiable financial information – stored by 'financial institutions', and by requiring financial institutions to provide notice of their information-sharing practices. In brief, the GLBA requires financial institutions: to provide notices of policies and practices regarding disclosure of personal information; to prohibit the disclosure of such data to unaffiliated third parties unless consumers are provided the right to opt out of such disclosure or other exceptions apply; and to establish safeguards to protect the security of personal information.

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003, imposes requirements on entities that possess or maintain consumer credit reporting information, or information generated from consumer credit reports. Consumer reports are 'any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility' for credit, insurance, employment, or other similar purposes. The FCRA mandates accurate and relevant data collection to give consumers the ability to access and correct their credit

12 Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices, available at www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf (last accessed 4 August 2014).

information, and limits the use of consumer reports to permissible purposes, such as employment and extension of credit or insurance.[13]

Health-care privacy

For health-care privacy, agencies within the Department of Health and Human Services administers and enforces the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). HIPAA was enacted to create national standards for electronic healthcare transactions, and the US Department of Health and Human Services has promulgated regulations to protect privacy and security of personal health information (PHI). Patients generally have to opt in before their information can be shared with other organisations.[14] HIPAA applies to 'covered entities', which include health plans, health-care clearing houses, and health-care providers that engage in electronic transactions as well as, via HITECH, service providers to covered entities that need access to PHI to perform their services. It also imposes requirements in connection with employee medical insurance.

'Protected health information' is defined broadly as 'individually identifiable health information […] transmitted or maintained in electronic media' or in 'any other form or medium'. 'Individually identifiable health information' is defined as information that is a subset of health information including demographic information that 'is created or received by a health care provider, health plan, employer, or health care clearinghouse'; and 'relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual' and either identifies the individual or provides a reasonable means by which to identify the individual. HIPAA also does not apply to 'de-identified' data.

A 'business associate' is an entity that performs or assists a covered entity in the performance of a function or activity that involves the use or disclosure of PHI (including, but not limited to, claims processing or administration activities). Business associates are required to enter into agreements, called business associate agreements, requiring business associates to use and disclose PHI only as permitted or required by the business associate agreement or as required by law, and to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate agreement, as well as numerous other provisions regarding confidentiality, integrity and availability of electronic PHI. HIPAA and HITECH not only restrict access to and use of medical information, but also impose stringent information security standards.

Communications privacy

For communications privacy, the Federal Communications Commission, the Department of Justice and, to a considerable extent, private plaintiffs can enforce the data protection

13 Available at www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act.

14 Available at www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf.

standards in the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and various Communications Acts, which include specific protection for 'customer proprietary network information' such as telephone call records.

The Electronic Communications Privacy Act of 1986 protects the privacy and security of the content of certain electronic communication and related records. The Computer Fraud and Abuse Act prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems, and can often be invoked against disloyal insiders or cyber-criminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks.

Children's privacy

COPPA applies to operators of commercial websites and online services that are directed to children under the age of 13, as well as general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. COPPA requires that these website operators post a privacy policy, provide notice about collection to parents, and obtain verifiable parental consent before collecting personal information from children, and other actions.[15]

Even the array of privacy laws described above is hardly comprehensive. A number of other federal privacy laws protect personal information in the areas of cable television, education, telecommunications customer information, drivers' and motor vehicle records, and video rentals. Federal laws also protect marketing activities such as telemarketing, junk faxes and unsolicited commercial e-mail.

State legislation

In the areas of online privacy and data security alone, state legislatures have passed a number of laws covering access to employee and student social media passwords, children's online privacy, e-Reader privacy, online privacy policies, false and misleading statements in website privacy policies, privacy of personal information held by ISPs, notice of monitoring of employee email communications and internet access, phishing, spyware, security breaches, spam, and event data recorders. California is viewed as the leading legislator in the privacy arena, with many other states following its privacy laws. State attorneys general also have concurrent authority with the FTC or other federal regulators under various federal laws, such as COPPA, HIPAA and others.

The National Council of State Legislatures summarises the following state provisions regarding online privacy:

> ***Privacy policies for websites or online services***
>
> *California's Online Privacy Protection Act requires an operator […] to post a conspicuous privacy policy on its Web site or online service […] and to comply with that policy. The law, among other things, requires that the privacy policy identify the categories of personally identifiable*

15 Available at www.law.cornell.edu/USCode/text/15/6501.

information that the operator collects about individual consumers who use or visit its Web site [and] how the operator responds to a web browser 'Do Not Track' signal. Connecticut [r]equires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy must be "publicly displayed" by posting on a web page and the policy must […] protect the confidentiality of Social Security numbers.

Privacy of Personal Information Held by Internet Service Providers

Two states, Nevada and Minnesota, require Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Both states prohibit disclosure of personally identifying information, but Minnesota also requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited.

False and Misleading Statements in Website Privacy Policies

Nebraska prohibits knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public. Pennsylvania includes false and misleading statements in privacy policies published on Web sites or otherwise distributed in its deceptive or fraudulent business practices statute.

Notice of Monitoring of Employee E-Mail Communications and Internet Access

Connecticut and Delaware require employers to give notice to employees prior to monitoring e-mail communications or Internet access.[16]

Children's online privacy

California prohibits websites directed to minors from advertising products based on information specific to that minor. The law also requires the website operator to permit a minor to request removal of content or information posted on the operator's site or service by the minor, with certain exceptions.[17]

IV INTERNATIONAL DATA TRANSFER

There are no significant or generally applicable data transfer restrictions in the United States.

The Federal Trade Commission is committed to international interoperability and cooperation. The US–EU Safe Harbor framework permits the FTC to complement the EU's effort to protect European consumers' privacy. The FTC has stated that Safe Harbor is a top enforcement priority.[18] The FTC has brought dozens of Safe Harbor

16 National Conference of State Legislatures, www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

17 Calif. Bus. & Prof. Code Sections 22580–22582.

18 Available at www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-USeu-safe-harbor-

cases,[19] and the agency is committed to review on a priority basis all referrals from EU Member State authorities. The agency only began receiving referrals in the past three years, and on its own initiative sought to identify Safe Harbor violations in every privacy and data security investigation it conducts. The resulting orders protect over a billion consumers worldwide, including millions of European citizens.

The FTC has signed a memorandum of understanding[20] with Ireland's Office of the Data Protection Commissioner in June 2013 to promote communication and cooperation between the two agencies in an era when consumer information is increasingly moving across borders. The FTC also signed a memorandum of understanding with the UK Information Commissioner's Office in March 2014.[21] The memorandum of understanding is designed to promote increased cooperation and communication in both agencies' efforts to protect consumer privacy.

In 2012, the United States was approved as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and the FTC became the system's first privacy enforcement authority. The FTC's Office of International Affairs[22] works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.[23] In particular, the FTC works extensively with the Global Privacy Enforcement Network and APEC.[24]

V COMPANY POLICIES AND PRACTICES

A recent study of corporate privacy management[25] reveals the success of enforcement in pushing corporate privacy managers to look beyond the letter of the law to develop state-of-the-art privacy practices that anticipate FTC enforcement actions, best practices, and other forms of FTC policy guidance. Many corporate privacy managers explain that the constant threat and unpredictability of future enforcement by the FTC and parallel state consumer protection officials, combined with the deterrent effect of enforcement

framework/131112europeancommissionsafeharbor.pdf.

19 See FTC Enforcement: Cases and Proceedings, available at www.ftc.gov/enforcement/cases-proceedings (last accessed 3 March 2014).

20 Press release, 'FTC Signs Memorandum of Understanding with Irish Privacy Enforcement Agency' (27 June 2013), available at www.ftc.gov/news-events/press-releases/2013/06/ftc-signs-memorandum-understanding-irish-privacy-enforcement.

21 www.ftc.gov/system/files/attachments/international-competition-consumer-protection-cooperation-agreements/140306ftc-uk-mou.pdf.

22 See FTC, Office of International Affairs, www.ftc.gov/about-ftc/bureaus-offices/office-international-affairs.

23 See FTC, International Consumer Protection, www.ftc.gov/policy/international/international-consumer-protection.

24 See 'APEC Overview', Chapter 2.

25 Bamberger, Kenneth A and Mulligan, Deirdre K, 'Privacy on the Books and on the Ground' (18 November 2011) *Stanford Law Review*, Volume 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385. Available at http://ssrn.com/abstract=1568385.

actions against peer companies, motivate their companies to proactively develop privacy policies and practices that exceed industry standards. Other companies respond by hiring a privacy officer or creating or expanding a privacy leadership function. The risk of enforcement also prompted companies to engage in ongoing dialogues with the FTC and state regulators.

Corporate privacy managers also emphasised that while compliance-oriented laws in other jurisdictions do not always keep pace with technological innovation, the FTC's Section 5 enforcement authority allows it to remain nimble in protecting consumer privacy as technology and consumer expectations evolve over time.

The United States does not require companies to appoint a data protection officer (although specific laws such as the GLBA and HIPAA require companies to designate employees to be responsible for the organisation's mandated information security and privacy programs). However, it is a best practice to appoint a chief privacy officer and an IT security officer. Most businesses in the US are required to take reasonable physical, technical and organisational measures to protect the security of sensitive personal information, such as financial or health information. An incident response plan and vendor controls are not generally required under federal laws (other than under the GLBA and HIPAA), although they are best practice in the US and may be required under some state laws. Regular employee training regarding data security is also recommended.

Some states have enacted laws that impose additional security or privacy requirements. For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and California requires covered entities to have an online privacy policy with specific features, such as an effective date.

VI DISCOVERY AND DISCLOSURE

Companies may be required under various federal and state laws to produce information to law enforcement and regulatory authorities, and to civil litigation demands. For example, companies may be ordered to produce information based on federal or state criminal authorities issuing a search warrant, a grand jury subpoena or a trial subpoena, or federal or state regulatory authorities issuing an administrative subpoena. Further, companies could be ordered to produce information upon receiving a civil subpoena in civil litigation.

Such US legal demands may create potential conflicts with data protection or privacy law outside the US. Companies should consider these possible conflicts when crafting their global privacy and data protection compliance programmes. Consideration should be given to whether US operations require access to European data, such that European data could be considered within the company's lawful control in the US and thereby subject to production requests irrespective of European blocking statutes.

The US does not have a blocking statute. Domestic authorities generally support compliance with requests for disclosure from outside the jurisdiction. The principle of

comity is respected, but national law and the Federal Rules of Civil Procedure typically trump foreign law.[26]

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Every business in the United States is subject to privacy laws and regulations at the federal level and frequently at the state level. These privacy laws and regulations are actively enforced by federal and state authorities, as well as in private litigation. The Federal Trade Commission, the Executive Branch and state attorneys general also issue policy guidance on a number of general and specific privacy topics.

Like many other jurisdictions, the United States does not have a central *de jure* privacy regulator. Instead, a number of authorities – including, principally, the Federal Trade Commission and state consumer protection regulators (usually the state Attorney General) – exercise broad authority to protect privacy. In this sense, the US has more than 50 *de facto* privacy regulators overseeing companies' information privacy practices. Compliance with the FTC's guidelines and mandates on privacy issues is not necessarily coterminous with the extent of an entity's privacy obligations under federal law – a number of other agencies, bureaus and commissions are endowed with substantive privacy enforcement authority.

Oversight of privacy is by no means exclusively the province of the federal government – state attorneys general have increasingly established themselves in this space, often drawing from authorities and mandates similar to those of the FTC. The plaintiff's bar increasingly exerts its influence, imposing considerable privacy discipline on the conduct of corporations doing business with consumers.

At the federal level, Congress has passed robust laws protecting consumers' sensitive personal information, including health and financial information, information about children, and credit information. At the state level, nearly all 50 states have data breach notification laws on the books,[27] and many state legislatures – notably California[28] – have

26 *Société Nationale Industrielle Aérospatiale v. US District Court*, 482 U.S. 522, 549 (1987) (requiring a detailed comity analysis balancing domestic and foreign sovereign interests, in particular US discovery interests and foreign blocking statutes). These issues are currently being litigated in a case involving execution of criminal search warrant issued to Microsoft for data stored in its servers located in Ireland. The case is now on appeal following a district court decision obliging Microsoft to produce the data in question.

27 See www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

28 See www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

passed privacy laws that typically affect businesses operating throughout the United States.[29]

Federal Trade Commission

The FTC is the most influential government body that enforces privacy and data protection[30] in the United States.[31] It oversees essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers.[32] Through exercise of powers arising out of Section 5 of the Federal Trade Commission Act, the FTC has taken a leading role in laying out general privacy principles for the modern economy. Section 5 charges the FTC with prohibiting 'unfair or deceptive acts or practices in or affecting commerce'.[33] The FTC's jurisdiction spans across borders – Congress has expressly confirmed the FTC's authority to provide redress for harm abroad caused by companies within the US.[34]

As FTC Commissioner Julie Brill has noted, 'the FTC has become the leading privacy enforcement agency in the United States by using with remarkable ingenuity, the tools at its disposal to prosecute an impressive series of enforcement cases.'[35] Using this authority, the FTC has brought numerous privacy deception and unfairness cases and enforcement actions, including over 100 spam and spyware cases and approximately 60 data security cases.[36]

The FTC has sought and received various forms of relief for privacy related 'wrongs' or bad acts, including injunctive relief, damages, and the increasingly popular practice of consent decrees. Such decrees require companies to unequivocally submit to the ongoing oversight of the FTC and implement controls, audits, and other privacy enhancing processes during a period of time that can span decades. These enforcement actions have

29 See, for example, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx and www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

30 This discussion refers generally to 'privacy' even though, typically, the subject matter of an FTC action concerns 'data protection' more than privacy. This approach follows the usual vernacular in the US.

31 See Daniel J Solove & Woodrow Hartzog, 'The FTC and the New Common Law of Privacy', 114 *Columbia L. Rev.* __ (forthcoming 2014) ('It is fair to say that today FTC privacy jurisprudence is the broadest and most influential force on information privacy in the United States—more so than nearly any privacy statute and any common law tort.'), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

32 See http://export.gov/static/sh_en_FTCLETTERFINAL_Latest_eg_main_018455.pdf.

33 15 U.S.C. Section 45.

34 15 U.S.C. Section 45(a)(4).

35 Commissioner Julie Brill, 'Privacy, Consumer Protection, and Competition', Loyola University Chicago School of Law (27 April 2012), available at www.ftc.gov/speeches/brill/120427loyolasymposium.pdf.

36 See Commissioner Maureen K Ohlhausen, 'Remarks at the Digital Advertising Alliance Summit' (5 June 2013), available at www.ftc.gov/speeches/ohlhausen/130605daasummit.pdf.

been characterised as shaping a common law of privacy that guides companies' privacy practices.[37]

'Deception' and 'unfairness' effectively cover the gamut of possible privacy-related actions in the marketplace. Unfairness is understood to encompass unexpected information practices, such as inadequate disclosure or actions that a consumer would find 'surprising' in the relevant context. The FTC has taken action against companies for deception when false promises, such as those relating to security procedures that are purportedly in place, have not been honoured or implemented in practice. As part of this new common law of privacy (which has developed quite aggressively in the absence of judicial review), the FTC's enforcement actions include both online and offline consumer privacy practices across a variety of industries, and often target emerging technologies such as the internet of things.

The agency's orders generally provide for ongoing monitoring by the FTC, prohibit further violations of the law, and subject the businesses to substantial financial penalties for order violations. The orders protect all consumers dealing with the business, not just the consumers who complained about the problem. The FTC also has jurisdiction to protect consumers worldwide from practices taking place in the US – Congress has expressly confirmed the FTC's authority to redress harm abroad caused from within the US.[38]

The states

State attorneys general retain powers to prohibit unfair or deceptive trade practices similar to the FTC arising from powers granted by 'unfair or deceptive acts and practices' statutes. Recent privacy events have seen increased cooperation and coordination in enforcement amongst state attorneys general, whereby multiple states will jointly pursue actions against companies that experience data breaches or other privacy allegations. Coordinated actions among state attorneys general often exact greater penalties from companies than would typically be obtained by a single enforcement authority. In the past two years, several state attorneys general have formally created units charged with the oversight of privacy, including states such as California, Connecticut and Maryland.

The mini-FTC Acts in 43 states and the District of Columbia include a broad prohibition against deception that is enforceable by both consumers and a state agency. In 39 states and the District of Columbia, these statutes include prohibitions against unfair or unconscionable acts, enforceable by consumers and a state agency.

ii Recent enforcement cases

FTC data protection enforcement

The FTC's data protection enforcement has spanned both privacy and security cases and has focused on both large and small companies across a variety of industries. Three illustrative cases are summarised below.

37 See, for example, Solove and Harzog, 2014 (footnote 31, *supra*).

38 15 U.S.C. Section 45(a)(4).

Internet of things

The FTC recently broke new ground by bringing an enforcement action in the emerging field of the internet of things. In September 2013, the FTC announced that it settled a case with TRENDnet, a company that markets video cameras designed to allow consumers to monitor their homes remotely. The FTC's complaint charged that the company falsely claimed in numerous product descriptions that its cameras were 'secure'; in reality, the cameras were equipped with faulty software that permitted anyone with the cameras' internet address to watch or listen online. As a result, hundreds of consumers' private camera feeds were made public on the internet. The FTC's order imposes numerous requirements on TRENDnet: a prohibition against misrepresenting the security of its cameras; the establishment of a comprehensive information security programme designed to address security risks; submitting to third-party assessments of its security programmes every two years for the next 20 years; notifying customers of security issues with the cameras and the availability of the software update to correct them; and providing customers with free technical support for the next two years.[39]

Online advertising

In December 2012, the FTC announced a settlement with a large online advertising company, Epic Marketplace Inc, that was using 'history sniffing' to secretly and illegally gather data from millions of consumers about their interest in sensitive medical and financial issues, from fertility and incontinence to debt relief and personal bankruptcy. The company would then use this information to send consumers targeted ads. The FTC's order barred the company from continuing to use the history sniffing technology and required it to destroy information that it had gathered unlawfully.[40]

Financial and medical information

In 2009 the FTC settled a case against CVS Caremark (CVS) the largest pharmacy chain in the United States, which had been charged with failing to take reasonable and appropriate security measures to protect the sensitive financial and medical information of its customers and employees, in violation of federal law. Based on its failure to take these measures, CVS was also charged with engaging in unfair and deceptive practices by failing to act in accordance with its claim that 'nothing is more central to our operations than maintaining the privacy of your health information'. The FTC order requires CVS to maintain a comprehensive information security programme; to obtain a biannual audit from an independent professional for the next 20 years; and remain subject to FTC monitoring. In a related settlement with the Department of Health and Human Services,

39 Press Release, 'FTC Approves Final Order Settling Charges Against TRENDnet, Inc.' (7 February 2014), available at www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

40 Press Release, 'FTC Approves Final Order Settling Charges Against Epic Marketplace, Inc.' (19 March 2013), available at www.ftc.gov/news-events/press-releases/2013/03/ftc-approves-final-order-settling-charges-against-epic.

CVS had to develop new policies and practices related to information handling; undergo outside auditing; and pay US$2.25 million to the agency.[41]

Safe Harbor enforcement cases

The FTC has pursued a number of enforcement actions against companies under its Safe Harbor authority.[42] The FTC's Safe Harbor cases allege both specific violations of the Safe Harbor's privacy principles and false claims of Safe Harbor participation, in which companies continue to represent themselves as Safe Harbor members even when their annual certifications have lapsed. US entities that persistently fail to comply with the Safe Harbor principles will lose the benefits of Safe Harbor participation.[43]

Mini-FTC Act privacy enforcement cases

In the past few years, state attorneys general have brought a number of enforcement actions pursuant to their authority under their respective states' mini-FTC Acts. Two illustrative examples are summarised below.

Google Street View settlement

Thirty-eight state attorneys general reached a US$7 million settlement with Google over allegations that the company violated people's privacy by collecting Wi-Fi data as part of its Street View activities. Google agreed to train its employees about privacy and confidentiality for at least the next 10 years and to destroy or secure any improperly collected information.[44]

Safari cookie settlements

In July 2013, the New Jersey Attorney General's Office announced a US$1 million settlement with online advertising company PulsePoint concerning allegations that the company bypassed web browser privacy settings to collect information on consumers'

41 Press Release, 'FTC Approves Final Consent Order in Matter of CVS Caremark Corporation' (23 June 2009), available at www.ftc.gov/news-events/press-releases/2009/06/ftc-approves-final-consent-order-matter-cvs-caremark-corporation.

42 See *In the Matter of Myspace LLC*, FTC File No. 102 3058 (2012); *In the Matter of Facebook, Inc*, FTC File No. 092 3184 (2011); *In the Matter of Google Inc*, FTC File No. 102 3136 (2011); *In the Matter of Collectify LLC*, FTC File No. 092 3142 (2009); *In the Matter of Progressive Gaitways LLC*, FTC File No. 092 3141 (2009); *In the Matter of Directors Desk LLC*, FTC File No. 092 3140 (2009); *In the Matter of Onyx Graphics, Inc*, FTC File No. 092 3139 (2009); *In the Matter of ExpatEdge Partners, LLC*, FTC File No. 092 3138 (2009); *In the Matter of World Innovators, Inc*, FTC File No. 092 3137 (2009); and *FTC v. Javian Karnani, and Balls of Kryptonite, LLC*, Civil Action No. 09-CV-5276, FTC File No. 092 3081 (2009).

43 US–EU Safe Harbor Framework: Guide to Self-Certification at 32.

44 See, for example the press release, 'Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data' (12 March 2013), available at www.ct.gov/ag/cwp/view.asp?Q=520518.

online browsing habits to serve millions of online advertisements.[45] In November 2013, 37 states settled an investigation with Google involving essentially the same allegations for US$17 million.[46]

iii Private litigation

Privacy rights have long been recognised and protected by common law. The legal scholar William Prosser created a taxonomy of four privacy torts in his 1960 article 'Privacy' and later codified the same in the American Law Institute's Restatement (Second) of Torts. The four actions for which an aggrieved party can bring a civil suit are intrusion upon seclusion or solitude, or into private affairs; public disclosure of embarrassing private facts; publicity which places a person in a false light in the public eye; and appropriation of one's name or likeness. These rights protect not only the potential abuse of information, but generally govern its collection and use.

The plaintiff's bar

The plaintiff's bar is highly incentivised to vindicate commercial privacy rights – through consumer class action litigation. The wave of lawsuits that a company faces after being accused in the media of misusing consumer data, or being victimised by a hacker or suffering a data breach incident, is well known across the country.

Role of courts

Courts remain central to defining and reshaping the contours of privacy rights and remedies. This role goes beyond the role of trial courts in adjudicating claims brought by regulators and private parties that seek to protect and define privacy rights and remedies; interest in these issues has been expressed at the highest levels. The Supreme Court has demonstrated recent interest on commercial privacy matters; in a November 2013 dismissal of a petition for certiorari, Chief Justice Roberts noted in dicta what issues the Court might consider when evaluating the fairness of class action remedies brought by plaintiffs challenging a privacy settlement.[47] Consumer protection regulators like the FTC and state attorneys general are becoming increasingly aggressive – both in terms of the scope of enforcement jurisdiction and the stringency of regulator expectations.

---

45 Press release, 'New Jersey Division of Consumer Affairs Obtains Million-Dollar Settlement With Online Advertising Company Accused of Overriding Consumers' Privacy Settings Without Consent' (25 July 2013), available at http://nj.gov/oag/newsreleases13/pr20130725a.html.

46 Press release, 'A.G. Schneiderman Announces $17 Million Multistate Settlement With Google Over Tracking Of Consumers' (18 November 2013), available at www.ag.ny.gov/press-release/ag-schnetiderman-announces-17-million-multistate-settlement-google-over-tracking.

47 Statement of Chief Justice Roberts, *Marek v. Lane*, 571 US ___ (2013).

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Foreign organisations can face a federal or state regulatory action or private action if the organisation satisfies normal jurisdictional requirements under US law. Jurisdiction typically requires minimum contacts with or presence in the United States. Additionally, a foreign organisation could be subject to sector-specific laws if the organisation satisfies that law's trigger. For example, if a foreign organisation engages in interstate commerce in the US, the FTC has jurisdiction. If a foreign organisation is a publicly traded company, the SEC has jurisdiction. If an organisation is a health-care provider, the Department of Health and Human Services has jurisdiction.

Additionally, foreign organisations must consider the residency of their data subjects. Massachusetts information security regulations apply whenever an organisation processes data of Massachusetts residents. Since Massachusetts was among the first states to enact information security requirements, it has become a *de facto* national standard.

The US does not have any forced localisation requirements for data servers, and national requirements have even been struck down in the government procurement context. Though the US does not force localisation, it requires vendor oversight to ensure reasonable standards of data care. A foreign organisation operating in the US should know they are the responsible party under US law, even if data processing is handled by a vendor outside the US.

The US does not have any jurisdictional issues for multinational organisations related to cloud computing, human resources and internal investigations. However, foreign organisations subject to US law should carefully consider how their data network is structured, and ensure they can efficiently respond to international data transfer needs, including for legal process. The US respects comity but a foreign country's blocking statute does not trump a US legal requirement to produce information.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity has been the focus of intense attention in the United States in recent years and the legal landscape is dynamic and rapidly evolving. Public discourse has tended to conflate distinct legal issues into a single conversation that falls under the blanket term 'cybersecurity'. Cybersecurity law and policy are more accurately described and characterised in distinct buckets primarily consumer or personal information, on the one hand, and critical infrastructure or sensitive corporate data on the other. Of course, the same or similar safeguards provide protection in both contexts.

While the United States does not have an omnibus law that governs data security, an overlapping and comprehensive set of laws enforced by federal and state agencies provides for the security of this information. These information security safeguards for personal and consumer information, as well as data breach notification provisions, are prescribed in the federal GLBA (financial data), HIPAA (health-care data), and 47 state laws plus the laws of numerous US territories and districts like the District of Columbia (for broad categories of sensitive personal information). The GLBA, HIPAA and Massachusetts

state law[48] provide the most detailed and rigorous information security safeguards. The emergence of the National Institute for Standards and Technology (NIST) cybersecurity framework, as detailed below, is likely to emerge as the predominant framework under which companies undertake to ensure information security.

Forty-seven states have enacted data breach notification laws, which have varying notification thresholds and requirements. These laws generally require that individuals be notified, usually by mail (although alternate notice provisions exist), of incidents in which their personal information has been compromised. These laws usually include a notification trigger involving the compromise of the name of an individual and a second, sensitive data element such as date of birth or credit card account number.

The GLBA Safeguards Rule requires financial institutions to protect the security and confidentiality of their customers' personal information, such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers. The Safeguards Rule requires companies to develop a written information security plan that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

a designate an employee to coordinate its information security programme;

b conduct a risk assessment for risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks;

c design and implement a safeguards programme, and regularly monitor and test it;

d select service providers that can maintain appropriate safeguards, contractually require them to maintain such safeguards, and oversee their handling of customer information; and

e evaluate and adjust the programme in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[49]

The Securities and Exchange Commission (SEC) has broad investigative and enforcement powers over public companies that have issued securities that are subject to the Securities Acts, and enforce this authority through the use of a number of statutes, including Sarbanes-Oxley. The SEC is currently investigating companies for alleged cybersecurity failures under two theories: (1) that material risks were not appropriately disclosed and reported pursuant to the agency's guidance on how and when to disclose material cybersecurity risk; and (2) that internal controls for financial reporting relating to information security did not adequately capture and reflect the potential risk posed to the accuracy of financial results. The SEC also enforces Regulation S-P, which

48 See Standards for the Protection of Personal Information of Residents of the Commonwealth (of Massachusetts], 201 CMR 17.00, available at www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

49 www.business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.

implements the privacy and security provisions of the GLBA for entities subject to its direct regulatory jurisdiction (such as broker-dealers and investment advisers).

The Department of Health and Human Services administers the HIPAA Breach Notification Rule, which imposes significant reporting requirements and provides for civil and criminal penalties for the compromise of PHI maintained by entities covered by the statute (covered entities) and their business associates. The HIPAA Security Rule also requires covered entities to maintain appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

Several states also require companies operating within that state to adhere to information security standards. The most detailed and strict of these laws is the Massachusetts Data Security Regulation, which requires that companies maintain a written information security policy (commonly known as a 'WISP') that covers technical, administrative and physical controls for the collection of personal information.

In February 2013, President Obama issued Executive Order 13,636, 'Improving Critical Infrastructure Cybersecurity'. This Executive Order directs the Department of Homeland Security to address cybersecurity and minimise risk in the 16 critical infrastructure sectors identified pursuant to Presidential Policy Directive 21.[50] The Order directed the NIST to develop a cybersecurity framework, the first draft of which was released in February 2014. The NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, and 'provides a means of expressing cybersecurity requirements to business partners and customers and help identify gaps in an organisation's cybersecurity practices'. While the framework is voluntary and aimed at critical infrastructure, there is an increasing expectation that use of the framework (which is laudably accessible and adaptable) could become a *de facto* requirement for companies holding sensitive consumer or business proprietary data. Companies operating in highly regulated industries such as the defence industrial base, energy sector, health-care providers, banks subject to detailed examinations by the Federal Financial Institutions Examination Council, or investment firms that are regulated by the Securities and Exchange Commission are subject to detailed cybersecurity standards.

Also, as detailed above, the FTC increasingly plays the role of *de facto* cybersecurity enforcement agency where consumer or personal information is involved. Based on Section 5 of the FTC Act, the Commission has stated that providing reasonable and appropriate information security is required as a 'fair' trade practice. State attorneys general, empowered pursuant to state-level mini-FTC Acts (see Sections VII.i and ii, *supra*) have taken a similar approach. Essentially every major data breach is investigated by the FTC and state attorneys general.

X OUTLOOK

There may be more and increasing convergence between US and EU privacy regimes than is commonly believed. Focus on data protection is unquestionably growing throughout the US, and unlike many other regulatory issues, privacy has not become mired in

50 Available at www.dhs.gov/critical-infrastructure-sectors.

Democrat–Republican partisan battles. And though the EU often disparages the US approach, in some ways the recent EU privacy proposal cuts some red tape and promotes streamlined EU-wide regulatory approvals. It also focuses more heavily on what has been a priority in the US, namely information security and data breach notification requirements. The EU's new proposal also seeks to encourage more enforcement and collective redress, like that seen from the FTC and state attorneys general and in private class actions.

No system of data protection anywhere in the world has produced more legal settlements, judgments, consent decrees and, perhaps most importantly, corporate compliance programmes that seek to protect and ensure privacy than the United States. Even though every Member State of the European Union has a data protection authority, they vary greatly in terms of aggressiveness and resources. Indeed, a recent study found that the very 'unpredictability' of FTC's broad mandate proves a stronger incentive to invest in privacy than the European regulators' more siloed mandate.[51]

The FTC noted in recent testimony to Congress that enforcement actions have focused on 'protecting financially distressed consumers from fraud, stopping harmful uses of technology, protecting consumer privacy and data security, prosecuting false or deceptive health claims, and safeguarding children in the marketplace'.[52] The FTC's approach to emerging issues can be informal and inclusive, allowing for productive working relationships that have helped shape the development of products and services in a way that protects consumers while allowing the government to better understand the technology. The use of public meetings and workshops, such as a November 2013 event on the internet of things, to help identify cutting-edge issues raised by technology, is an example of such an approach.[53] The FTC has noted that issues likely to capture their privacy-related attention in the years ahead include big data, mobile technologies and connected devices, and protection of sensitive data, particularly health information and information that relates to children. Entities known as 'data brokers' have captured the attention of the FTC and Senator Rockefeller, and are likely to be targets for future enforcement and oversight. If nothing else, the robust public debate surrounding these issues is indicative of engaged, capable policymakers. Companies have responded to regulation and oversight by expanding privacy leadership functions, redoubling compliance and training efforts, and engaging in proactive and ongoing dialogues with federal and state regulators.

At the same time, cybersecurity has been an issue of intense focus for the government and private sector alike. This trend is likely to intensify in the coming years, as technology develops and changes and puts further strain on existing laws. Congressional gridlock has stymied reform on otherwise non-partisan issues, but as the post-Snowden clamour begins to fade, it is possible that legislation will come to pass to enable further

51 Bamberger and Mulligan, 2011 (see footnote 25).

52 Id.

53 Prepared Statement of the Federal Trade Commission on 'The FTC at 100: Where Do We Go From here?' before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade (December 2013).

collaboration between the private and public sector, and provide clearer reporting and notification requirements, eclipsing the messy state model that exists and is in use today.

Issues related to intellectual property theft are likely to continue to rise to the top of the international diplomacy agenda for the United States as its competitive position risks erosion from China and other such alleged cyber-intruders. Surveillance issues are likely to continue to be a sticking point between US and European counterparts, as even as Snowden fades, the explosion of cloud data centres is likely to continue to prove a point of tension with regard to requests for information by the United States government.

Investment in protection of computer and communications systems is likely to be a continued regulatory focus, as agencies – and companies – seek to determine and understand how to balance the costs and benefits of imposing information security requirements and reporting. Moreover, implementation of the NIST cybersecurity framework may emerge as a *de facto* requirement for companies. While the broader cybersecurity outlook is unclear, it is certain that intervening factual and technological developments will continue to propel this field to the front of the national consciousness – for reasons related to surveillance, competitiveness and intellectual property theft, or personal security when information is compromised (such as through retail breaches).

Appendix 1

ABOUT THE AUTHORS

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and lead global coordinator of Sidley Austin LLP's highly ranked privacy, data security and information law practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. Mr Raul's practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chairman of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Privacy, Intellectual Property, Technology and Antitrust Litigation Advisory Committee of the National Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President. He is a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government, and Yale Law School.

TASHA MANORANJAN

Sidley Austin LLP

Tasha Manoranjan is an associate in Sidley Austin's Litigation practice in the Washington, DC office, frequently supporting the privacy, data security and information law practice group. Ms Manoranjan earned her law degree at Yale Law School, where she served as the features editor and book reviewer for the *Yale Journal of International Law*, chair of the South Asian Law Students Association and community enrichment chair of the Women

of Color Collective. While at Yale, Ms Manoranjan wrote a paper entitled 'Beaten but not Broken: Tamil Women in Sri Lanka', which was subsequently published at 11 *Georgetown Journal of International Affairs* 139 (2010). Ms. Manoranjan received her BA, *magna cum laude*, in justice and peace studies from Georgetown University's School of Foreign Service. Before joining Sidley, Ms Manoranjan worked at the Department of Justice Human Rights and Special Prosecutions Section and at an advocacy group working on human rights in Sri Lanka.

VIVEK MOHAN

Sidley Austin LLP

Vivek Mohan is an associate with Sidley Austin LLP's privacy, data security and information law group in Washington, DC. Vivek is affiliated with and serves as visiting faculty for 'The Cyber Project' at the Harvard Kennedy School, where he spent two years as resident fellow. Vivek has also held a special appointment with the Internet Bureau of the Office of the New York State Attorney General and worked as in-house counsel at Microsoft's Innovation & Policy Center. Vivek holds a JD from Columbia University School of Law and a BA from the University of California, Berkeley.

SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com
tmanoranjan@sidley.com
vivek.mohan@sidley.com

www.sidley.com

Virginia's Cyber Security Approach:

Leadership through Diversity

The organizations that created the Internet four decades ago, the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation, are located in Virginia. Since the inception of the Internet, Virginia has been a focal point for the Internet and associated industries, with the majority of the Internet's traffic passing through its geographical borders. Today, the Commonwealth is home to more than 650 cyber security companies, the most per capita in the nation. Thousands of Virginians work on cyber security every day in corporations, universities, the military, the intelligence community, and in Commonwealth agencies.

The Commonwealth of Virginia continues to drive the development of new products, companies and services in the cyber security industry, underscored by its unique and abundant technology resources and leadership throughout the United States. Virginia has developed a world leading technology ecosystem founded on private industry innovation and public-private partnerships. By incorporating principles of collaboration, coordination, government involvement and investment, and integration across key markets, Virginia has created the best environment for cyber security research and development in the United States.[1]

Since the beginning, policymakers in the Commonwealth have understood that technology does not evolve in a vacuum, isolated from other innovations and without policy support. By leading the nation in the adoption of industry best practices, Virginia is a nationally recognized trailblazer that has consistently served as a both a driver and early-adopter of the best cyber security technologies available.[2] As the Commonwealth moves forward, its vision is not only to continue to lead the nation in the adoption of signature Information Communication Technologies (ICTs), but to help formulate and promote their creation through innovation, investment, and a pro-business environment that nurtures all companies.

The wealth of resources that have made Virginia a leader in innovation and technology are fueling the development of a new crop of cyber security solutions. In Virginia, this principle of integrated leadership is at the root of its economic success. Leaders from business, government, and higher education have co-created an environment that nurtures the types of innovation that have made the Commonwealth the home of the top technology companies and the number one recipient of federal investment. A shared vision for pro-business policies, a massive and highly skilled workforce and cutting-edge technology research has also planted Virginia at the heart of the cyber security space.

Leaders from business, government and education sectors come together to create network nodes for success – public-private partnerships that provide investment and thought leadership in the interest of cultivating and promoting technology companies. These relationships have continued to drive the performance of key technology firms, and maintained Virginia's leadership in the defense and technology space. Recognizing the need for ongoing development, the Commonwealth continues to adopt a "**collaborative security model**" recommended by leading major internet security firms that promote shared knowledge while protecting Intellectual Property (IP).[3]

Virginia continues to attract top technology firms through defense focused partnerships, leading the nation in federal defense investment.[4] A shared vision for pro-business policies, massive and highly skilled workforce that continue to grow through specialized programs at the many higher-education universities, and bleeding-edge technology research made possible through continued infrastructure development cultivate the best environment for developing cyber security technology.[5]

Cyber Security: The Crossroad of Prosperity and National Security

Cyber security is not a fad or fleeting challenge with a potential to crash in the future. Business, government, and citizens are more interconnected than ever, which has led both to great efficiencies and significant vulnerabilities that must be faced at all levels of society. The very way consumers and citizens interact with technology and society have likewise evolved to include significantly greater use of smartphones, tablets, and non-traditional computers, creating vulnerabilities that attackers are already eyeing. Everything from interconnected Barbie™ dolls and skateboards to autonomous connected cars and medical devices were hacked this year, highlighting the increased need for security and innovation to keep pace with the rapidly evolving threats.[6]

The need to maintain a protected cyber front is now considered a pillar of society as it protects vital infrastructure, secures privacy, ensures economic efficiency, and enables the most basic needs of society including water, gas, electricity, and finance. In fact, the President of the United States declared, "America's economic prosperity, national security,

[1]Sorcher, Sara. The Race to Build the Silicon Valley of Cybersecurity. http://passcode.csmonitor.com/goldrushAccessed June 9, 2016
[2]Spidalieri, Francseca. State of the States on Cybersecurity. Pell Center for International Relations and Public Policy. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdfNovember 2015
[3]http://www.internetsociety.org/globalinternetreport/?gclid=CjwKEAjw4dm6BRCQhtzI6Z6N4i0SJADFPu1ngr-3sRJqBidq2awzkE7SGGgT27n1td2xXR5q4GvwuxoC5hrw_wcB
[4]Burnell, Susan. Virginia: Investing in Innovation. Forbes.com. Oct. 20, 2014. http://custom.forbes.com/2016/01/27/virginia-investing-in-innovation/
[5]http://www.yesvirginia.org/cybersecurity
[6]https://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/

and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property."[7]

Simply put, as the world economy and governance infrastructure increasingly rely on Internet and cyber networks for greater efficiencies, these same efficiencies promote vulnerabilities and access points for new attacks, greater threats, and unknown resource vulnerability.[8] The internet user base has more than doubled since 2008, representing growth from roughly 1.4 billion users to 3.1 billion users in 2015, while the "touch points" for attacks have grown tremendously in the mobile sector.[9] Attacks over the last decade have evolved tremendously and will continue to evolve as the number of internet users grows, avenues of attack are closed and adversaries adapt, and as governments and private industry become more interconnected. The problem is not going away, and Virginia is leading the charge against these highly adaptive, international foes.

Government

Both national and state governments recognized throughout the 1990s and early 2000s that the Internet could serve as a catalyst for economic growth, development, and the championing of fast, reliable, and affordable communications—driving job creation, information access, and innovation. However, it is only recently that those same governments recognized the exposure and costs of less resilient critical services, disruption of services, e-crime, identity theft, intellectual property theft, fraud, and other malicious cyber activities in terms of economic loss and threat to people's safety and well-being.[10]

A 2014 Deloitte-NASCIO (National Association of State Chief Information Officers) study on cybersecurity issues revealed that states have been victims of a number of high-profile attacks that "have resulted in the loss of Personally Identifiable Information (PII) of millions of citizens, including Social Security Numbers, payment card records, dates of birth, driver's license numbers, and tax data…." The study recommended that "Critical Infrastructure Security and Resilience… should be a shared responsibility between all levels of government and the operators of critical infrastructure."[11] This collaborative and cooperative model of shared security and resilience has only been developed and adopted by a few leading states; Virginia among the first.

This collaborative and cooperative model of shared security and resilience has only been developed and adopted by a few leading states; Virginia among the first.

It is imperative that the Commonwealth of Virginia protects citizen data and provides a safe, secure technology environment that enables state agencies to accomplish their respective missions. To fulfill this task, the Virginia Information Technologies Agency (VITA) established the Commonwealth Security & Risk Management Directorate.

This Directorate develops and manages an ever-changing portfolio of tools and processes designed to secure Commonwealth data and systems. Principle among these is the establishment of a Shared Security Model. The Virginia General Assembly approved funding to establish shared services for delivery of cyber security functions to agencies and support vulnerability scanning of public facing websites.

Business

In 2015, there were an average of 160 successful cyber attacks per week against businesses in the United States, more than triple the 2010 mark of approximately 50 per week. At the same time, the cost of cyber crime in the United States more than doubled from $6.5 million in 2010 to $15.4 million in 2015 per company affected, with the largest attack reaping $65 million in damages.[12]

The threat of cyber attacks impacts every nation and every aspect of the world economy, and threats to national security and economic order continue to grow as internet use, interconnected activity, and the development of the Internet of Things (IoT) (the network of physical devices, vehicles, buildings and other items to be sensed and controlled remotely across existing network infrastructure) represent greater "touch points" and networked nodes to access.

This growth trend is likely to slow over the next five years, however growth will accelerate in China, India, and across African nations where most cyber attacks have originated from abroad, and the growth in mobile penetration across nations will continue to increase rapidly.[13] As computing and communications technologies become more entrenched in the global economy and IoT provides gateways to new data modes, incentives

[7]Obama, Barack. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity
[8]Zetter, Kim. The Biggest Security Threats We'll Face in 2016. 01/01/2016
[9]http://www.kpcb.com/internet-trends
[10]Hathaway et al, "Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index," Potomac Institute for Policy Studies, (forthcoming)
[11]Deloitte-NASCIO, "2014 Deloitte-NASCIO Cybersecurity Study"
[12]http://www.heritage.org/research/reports/2015/11/cyber-attacks-on-us-companies-since-november-2014
[13]http://resources.infosecinstitute.com/the-most-hacker-active-countries-part-i/

to compromise the security of these systems will likewise grow rapidly.[14]

The Virginia Story

Ranked consistently near the top in *Forbes'* annual list of Best States for Business, Virginia provides a wealth of opportunities, a great atmosphere for development and expansion, and leadership that truly understands the importance of maintaining the best business environment for economic prosperity. A variety of performance-based incentives, from tax credits to tax exemptions, are Virginia's investment in its economic future. The Commonwealth works enthusiastically with new and expanding employers who demonstrate a willingness to invest in those who invest in Virginia, create a high standard of living for Virginians, and enhance local and state economies through increased revenue growth.

Pro-Business Advantages for Companies

- Strategic East Coast location and excellent infrastructure provide easy access to national and global markets
- Stable, low tax costs for corporations and individuals and a 6% corporate income tax
- Minimized payroll costs with low worker's compensation rates and a low unemployment tax
- Favorable business environment that protects "at-will" and "right-to-work" employment practices
- One of the highest-ranked states in high-technology employment
- 38 established Technology Zones
- A vibrant and diverse multi-cultural community where employees can live and work

Photo by Matheus Gonçalves

National Cyber "Firsts" are Second Nature in Virginia

- National Institute of Standards and Technology (NIST) Cyber Framework: First in the nation to adopt federal standards
- Information Sharing and Assessment Organization (ISAO): First state to declare itself an ISAO
- Securing Consumer Transactions: First state to require security on debit or credit card present transactions, via Executive Directive #5
- Digital Identity: First state to enact landmark legislation, now used as the model by other states

- An experienced, educated and productive workforce
- Recruitment and training programs to help businesses become operational faster and maintain their competitive advantage
- More than 2,300 qualified buildings and sites located across the Commonwealth

The New Virginia Economy

In 2014, Virginia Governor Terry McAuliffe established the New Virginia Economy Workforce Initiative. This initiative seeks to overhaul our economy in four ways: increasing postsecondary education and workforce credentials, securing employment for veterans, aligning education with the needs of businesses, and diversifying the economy.

The Initiative seeks to better align workforce supply to employer demands and to ensure that Virginia's workers have the tools they need to succeed in a 21st century economy. The Initiative includes several ambitious goals, such as the "Pathway to 50K" initiative that sets a target of 50,000 credentials, licensures,

[14]Spidalieri, Francseca. State of the States on Cybersecurity. Pell Center for International Relations and Public Policy. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdfNovember 2015

apprenticeships, and sub-baccalaureate degrees earned that meet the immediate needs of Virginia's workforce.

Virginia's Leadership in Cyber Security

The Commonwealth of Virginia is a leading cyber security entity not only in its adoption and application of industry best practices, but also in the support and innovation environment growing new companies and new technologies. In a study by the Pell Center released in November 2015, *State of the States on Cybersecurity*, Virginia was recognized for its prioritization of the "importance of cyber security, chiefly by prioritizing their state's security and development strategy and through their commitment to increasing their resilience to cyber threats."[15]

The study demonstrated that Virginia is among the leaders in the nation for devising "innovative ways to raise awareness and implement creative solutions to protect state governments and their constituencies... highlighting leading best practices and efforts at the state level to adopt comprehensive cyber security policies and strategies, increasing funding and education, and developing programs to attract and retain qualified talent."[16]

Virginia was among the first states in the nation to adopt National Institute of Standards and Technology (NIST) special publications and benchmarks, such as International Organization for Standardization (ISO 27001 and 27002) and the Control Objectives for Information Technology (CoBIT), to secure data centers and information pipelines.[17] The cyber security mission is driving success across industries, through partnerships and relationships with federal and state governments, and enabled by a top pro-business environment.

SPOTLIGHT: The Interconnected World-Leading Innovation in Virginia

As governments and companies migrate their data to collocated centers hosted and secured by third party companies who specialize in proprietary and confidential data management, a major industry has located and propagated in Virginia. It is estimated, because of this new demand, that 70 percent of the world's internet traffic passes through Virginia largely due to the 60 data centers throughout the Commonwealth.

Recognizing this new opportunity and need, the Commonwealth embraced this flourishing market by passing tax exemptions to companies that buy or lease at least $150 million in computer equipment (between July 2010 and June 2020) for use in data centers. Major investments from Amazon, Microsoft, Bank of America, Northrop Grumman, Google, and others have accounted for over $9 billion and 7,600 new jobs since 2005 specifically in the development of data centers in Virginia. In 2014 alone, Microsoft announced a plan to expand their $500 million data center by $350 million in Boydton, Virginia offering excellent opportunities to the small town.[18]

The presence and density of these many data centers provide internet traffic security and housing that serve the national capital needs and the federal government. The needs of these unique users foster continued growth and demand in the cyber security space specifically, and related technologies more generally. Shared leadership across sectors has created an ecosystem where established enterprises can thrive while new start-ups innovate to solve newly evolving problems.

The IoT, interconnected devices that transcend computers or mobile phones and integrated across platforms, represents one of these new challenges being addressed in the Commonwealth by both established leaders such as GE and start-ups like AconAI. Accelerators and universities are turning out entrepreneurs addressing the next generation of security needs; Virgil Systems and Eunomics, both start-ups of MACH37, are good examples of how new and diverse technologies grow in the Virginia economy to meet the demands rising from IoT devices.

[15] Ibid Pg 4
[16] Ibid Pg 4
[17] Spidalieri, Francseca. State of the States on Cybersecurity. Pell Center for International Relations and Public Policy. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdfNovember 2015
[18] http://www.datacenterknowledge.com/archives/2014/06/13/microsoft-kicks-350m-data-center-expansion-virginia/

Photo by Norfolk State University

Virginia Cyber Security Commission

Within weeks of coming into office, Governor Terry McAuliffe established the Virginia Cyber Security Commission to both prepare and protect the Commonwealth of Virginia from cyber threats, as well as lay the policy framework that would allow Virginia to provide an excellent regulatory environment for firms working in the cyber security industry. From the beginning, the Commission concentrated efforts on building a cyber-ecosystem in Virginia across five areas – Education/Workforce, Economic Development, Awareness, Infrastructure, and Crime. The commission relied on Virginia's leadership, both public and private, and was co-chaired by Richard Clarke of Good Harbor Security Risk Management and Virginia Secretary of Technology Karen Jackson.

While recognized for its overall protection of state government and private enterprise through the work of the Commission, Virginia has invested in a number of strategic platforms that provide security and resilience to business, education, and governance. Among these industry-leading methodologies is to create and implement a State Cyber Security Strategic Plan, outline vital Incident Response Mechanisms, support E-Crime Law Enforcement, cultivate Information Sharing, and lead the nation in Cyber R&D, Education, and Capacity Building.

These five elements gave foundation to the internationally recognized structure for approaching cyber security threats and opportunities. Highlighting these five core elements of cyber security and resilience, the Commonwealth of Virginia Cyber Security Commission pointed to the following achievements in an August 2015 report:

- Became the first state to adopt the NIST Cyber Framework, issued by the President in Executive Order 13636, to provide guidance and a standard for organizations to achieve an effective cyber security posture
- Passed landmark legislation on Digital Identity (SB 814) which now serves as a model for other states and national governments
- Led the nation as the first state to embrace of the Information Sharing and Assessment Organization standard issued by the President in Executive Order 13691
- Established accountability and authority for cyber security in Commonwealth agencies through the passage of new legislation on the role of agency heads (SB 1121)
- Led the states in the adoption of the Advanced Credit Card Standard for security (Executive Directive 5)
- Led the states in the adoption of the Advanced Credit Card Standard for security (Executive Directive 5)
- Passed seven pieces of legislation that improve the ability of the Commonwealth to prosecute cyber-crime and develop cyber security policies[19]

A link to the Commission report can be found here: http://cyberva.virginia.gov/cyber-security-commission

[19]Commonwealth of Virginia Cybersecurity Commission. "Threat and Opportunities" August 2015 - https://cyberva.virginia.gov/media/4396/cyber-commission-report-final.pdf

Members of the Commission

Ms. Karen Jackson, *Co-chair, Virginia Secretary of Technology*

Mr. Richard A. Clarke, *Co-chair, Chairman and CEO of Good Harbor Security Risk Management*

Ms. Rhonda Eldridge, *Director of Engineering at Technica Corporation*

Ms. Jennifer Bisceglie, *President and CEO, Interos Solutions, Inc.*

Mr. Paul Kurtz, *Chief Strategy Officer at CyberPoint*

Mr. Paul Tiao, *Attorney and partner with the international law firm of Hunton and Williams, LLP*

Dr. Barry Horowitz, *Munster Professor of Systems and Information Engineering and Chair of the Systems and Information Engineering Department at the University of Virginia*

Mr. Andrew H. Turner, *Former Senior Vice President and Head of Global Security, VISA*

Ms. Jandria Alexander, *Principal Director of the Cyber Security Subdivision in the Engineering Technology Group at the Aerospace Corp*

Ms. Elizabeth "Betsy" Hight, *Retired US Navy rear admiral who served as the Vice Director of the Defense Intelligence Agency (DISA)*

Mr. John Wood, *Chief Executive Officer, Chairman of the Board, and Director for Telos Corporation*

Ms. Anne Holton, *Secretary of Education*

Mr. John Harvey, *Secretary of Veterans and Defense Affairs*

Dr. Bill Hazel, *Secretary of Health and Human Resources*

Mr. Maurice Jones, *Secretary of Commerce and Trade*

Mr. Brian Moran, *Secretary of Public Safety and Homeland Security*

SPOTLIGHT: MACH37 Cyber Accelerator

Nothing exemplifies Virginia's approach to cyber security support greater than the MACH37™ Accelerator – an intensive 90-day program created to launch cyber startups – headquartered at Virginia's Center for Innovative Technology (CIT) in Herndon, VA. Founded by the CIT and funded by the Virginia General Assembly, The Accelerator is designed to facilitate the creation of the next generation of cyber security product companies through mentorship, partnership, and cooperation.

Known as America's premier market-centric cybersecurity accelerator, the program facilitates the creation of next generation cybersecurity product companies with emphasis on the validation of product ideas and the development of relationships that produce an initial customer base and investment capital.[20] MACH37 Cyber Accelerator has graduated 35 new cyber companies (as of 4/1/16) and has two private sector investors (General Dynamics Mission Systems and Amazon Web Services).

MACH37's unique program design places heavy emphasis on the validation of product ideas and the development of relationships that produce an initial customer base and investment capital. The accelerator is operated by MACH37 partners who announced the latest addition, Amazon Web Services, at the highest level of partnership. Other partners include General Dynamics, Activate, Microsoft BizSpark, Rackspace, Square1bank, and Virtru who all help pick which companies are accepted to the program based on their technology, mission, and team.

While promoting robust industry relationships and cross-industry strategies, MACH37 takes cyber security start-up dreams and turns them into realities, driven by free-market economic challenges and helped along by small business support and investment from government. Virginia is leading this wave of innovation by bringing together private industry with government resources, and enabling industry to lead the discussion.

[20]https://www.mach37.com/explore/cohort-companies/

Virginia Cyber Security Partnership

Established in 2012 through a partnership with the FBI, the Virginia Cyber Security Partnership is a collaboration between public and private sectors designed to establish trust for combating Cyber threats. The Partnership has more than 220 active members, and has held more than 35 events throughout the Commonwealth.

The mission of the Virginia Cyber Security Partnership (VCSP) is to establish and maintain a trusted community of public and private sector cyber professionals. The Partnership leverages a collective experience and knowledge, promotes mutually beneficial information sharing and fosters professional development. This mission seeks to advance our nation's interests.

The VCSP has three primary mission objectives to support short-term and long-term goals:

Skills Enhancement

This mission objective is focused on providing opportunities to sharpen existing skillsets and develop new skills within cyber security. This will be accomplished through workshops, curriculum road maps, etc.

Outreach and Pipeline Development

This mission objective is focused on enhancing the awareness of cyber security and sharing opportunities within the cyber profession to help with enhancing the pipeline of skilled professionals to aid in cyber security. This will also include connecting strong candidates to potential employers.

Collaboration

This mission objective fosters community and strengthens the overall program by creating opportunities for members to collaborate on cyber related activities. This may include networking, outreach, workshops, portal communications, information sharing, etc.

Public Safety

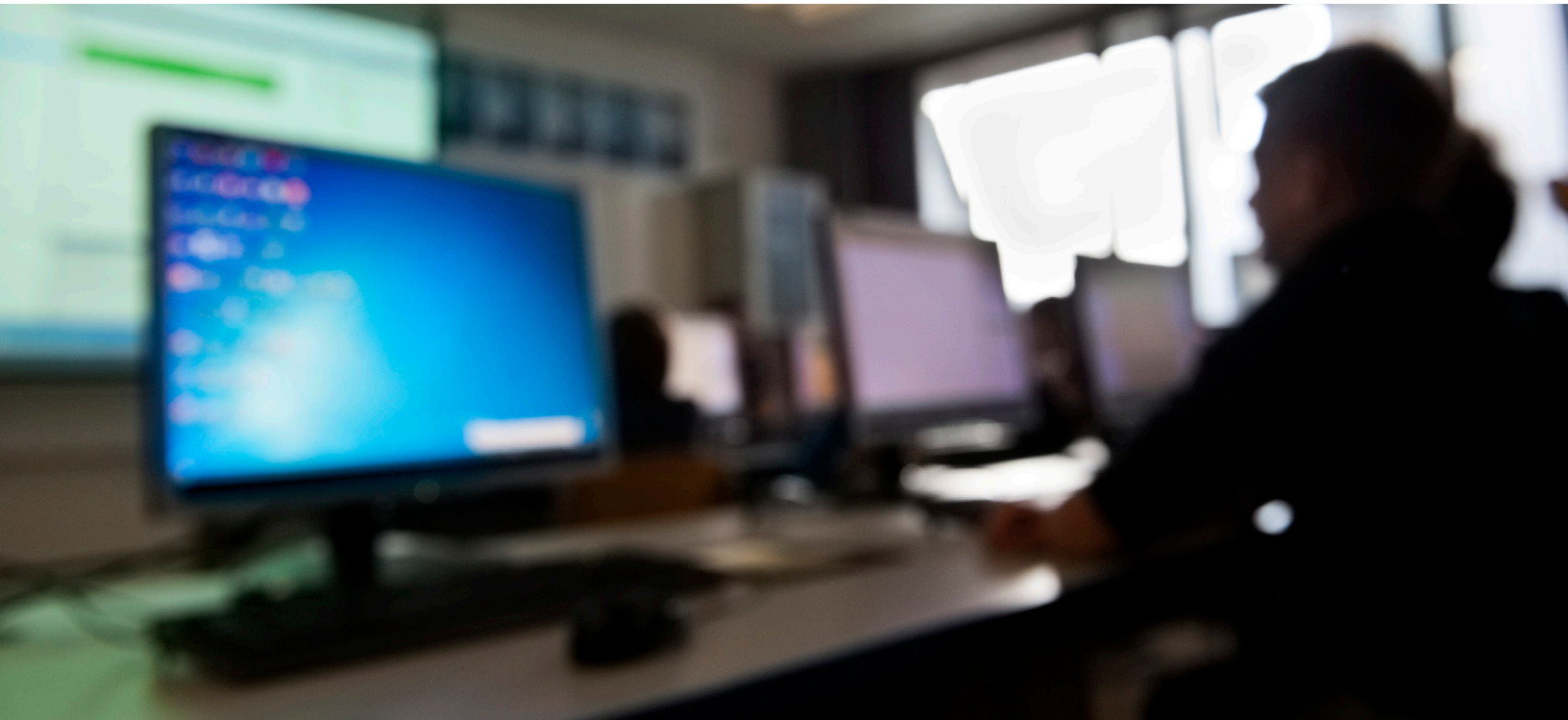
The Virginia Fusion Center

The Virginia Fusion Center (VFC) operates as a focal point within Virginia for the collection, receipt, analysis, and dissemination of timely threat intelligence between the federal government and state, local, and private sector partners. The VFC strives to operate under an all-hazards approach to threat information, and has developed cyber capabilities utilizing a civilian analyst and sworn special agents detailed from other mission areas to address ongoing cyber activities. These personnel identify and track known and emergent cyber threats to the Commonwealth in support of statewide awareness, detection, analysis, and response through the dissemination of timely and actionable cyber threat intelligence.

The VFC also provides analytical case support on criminal investigations with a cyber nexus, cyber security training and awareness, and increased cyber resilience through exercise and assessment. In 2014, the VFC produced 43 products related to potential cyber threats and cyber security. In 2016, the Virginia General Assembly funded four additional positions for the VFC.

Virginia State Police High Tech Crime Division (HTCD)

HTCD was formed within the Bureau of Criminal Investigation (BCI) in 2009 by the Department of State Police. The HTCD engages the use of leading technologies to proactively provide



specialized law enforcement services in support of the Department's overall mission. In 2016, the Virginia Assembly funded 10 additional positions within the HTCD. Key capabilities include:

- Investigation of "All Forms of High Tech Crimes"
- Investigation of Crimes Against Children
- Computer forensic laboratory services
- On-scene digital forensic services
- Technical support to federal, state, and local agencies
- Domestic, federal, and international agency liaison

Cyber Guard Prelude

Cyber Guard prelude 2015 was a table top exercise that engaged state agency partners as well as local, federal, and private sector stakeholders to test state level cyber response procedures. Planning is underway for a functional exercise, Cyber Guard 2016.

Virginia National Guard

Building on the efforts and recommendations of the Cyber Security Commission, Virginia is currently partnered with the Virginia National Guard's Data Processing Unit (DPU), capitalizing on the cyber security recommendations to utilize local assets such as the Guard to strengthen the Commonwealth's cyber infrastructure. The partnership conducts cyber assessments on infrastructure within Virginia localities to identify any gaps or opportunities to increase our cyber resilience. Upon completion of the assessment a detailed confidential after-action report is shared with the locality. As of July 2016, three missions have been completed, with an additional six identified in the near-term. Virginia's proactive stance in addressing cyber security has also led the Air National Guard to select Virginia as a location for their cyber-guard unit.

Workforce and Education

Technology companies are supported in Virginia by infrastructure that outperforms other states, and a pro-business environment geared toward innovation and IP-protection. They are also supported by a robust, educated, and well-developed workforce and a world-leading university system that produces thousands of graduates in cyber-related fields annually.

For cyber security firms looking to find the best workers and students in the nation to innovate and succeed, they need look no further than the Commonwealth of Virginia. This pipeline begins with K-12 education and continues through the Commonwealth's world-class post-secondary institutions, which include 13 National Centers of Academic Excellence at 11 institutions and produce more than 2,150 technology graduates annually.

Workforce

Maintaining a highly skilled workforce is a fundamental component to ensuring future success. As Virginia has led the nation in the adoption of vital protections for infrastructure and data security—creating one of the most vibrant, protected, and diverse technology ecosystems in the world—it has also been focusing on creating a specialized workforce through its nationally ranked public and private education system through funding, investments, and public-private partnerships. Virginia has the *largest concentration of high-tech workers in the United States*, with 9.8 percent of the state's private sector workforce in tech.[21] In 2014, 19.3 percent of Virginia's payroll came from technology companies.[22]

Veterans Pathway Program in Cyber Security (George Mason University): Supports student success through expanding a program that allows veterans who complete an Associate Degree at a Virginia community college to transfer (through guaranteed admissions) to GMU and earn a B.A.S. in Cyber Security

Virginia currently has more than 67,850 people working in cyber security alone, and many of Virginia's universities are at the forefront of cyber security research and development. Virginia's population of more than 8.2 million and a workforce of more than 4.2 million boasts the 8th highest education rate in the nation for those with a minimum of a bachelor's degree at 35 percent. Approximately 18,000 people leave Virginia military bases seeking civilian employment annually.

- Virginia currently supports the third highest concentration of technology jobs as a share of overall private-sector employment

[21] TechAmerica Foundation's annual Cyberstates Report
[22] http://www.doe.virginia.gov/administrators/superintendents_memos/2016/040-16a.pdf

- More than 35% of Virginians have at least a bachelor's degree, the 8th highest rate in the country
- More than 1,400 doctorate degrees in science and engineering are awarded annually from Virginia universities
- More than 15,000 science and engineering graduate students pursue advanced degrees in Virginia
- Approximately 18,000 people leave Virginia military bases each year and enter the civilian workforce

This workforce includes the high-tech skills found in our northern Virginia Technology Corridor, highly skilled veterans returning to civilian life from one of the many regional defense installations, and leading edge research performed at our universities and local federal laboratories.

Cyber Security Apprenticeship Program

Starting in June of 2016, businesses have the opportunity to stand up registered apprenticeships for cyber security occupations. Formally approved by the Virginia Apprenticeship Council, the three new registered apprenticeship cyber security occupations include: Information Security Analyst - Cyber Security Analyst, Information Security Analyst - Computer Forensics Analyst, and Information Security Analyst - Incident Response Analyst.

Introducing registered apprenticeship occupations in an industry sector like cyber security that has not traditionally employed apprentices will boost the ability of young adults and career switchers to attain in-demand skills and even earn industry certifications and college credits. These programs bolster Virginia's national leadership in cyber education and training and lay a firm foundation for this emerging sector.

Education

cyber.virginia.gov/doe

The Commonwealth's commitment to integrating cyber security into education pathways has already begun. The Cyber Security Commission hosted the Commonwealth Conference on Cyber and Education 2015 on December 2, 2015, to engage educators, employers, and government in a dialogue on cyber security.

As one result, the Virginia Department of Education established Cyber Security as a career pathway that begins with career and technical education programs in middle grades and high schools.[23] This includes the creation of Virginia's Cyber Security and Cyber Forensics Infusion Units, which have identified eighty-five tasks/competencies that can be incorporated into existing technology or STEM courses. Included are Basic Operations and Concepts, Social and Ethical Issues, Technology Research Tools, Thinking Skills, Problem Solving and Decision Making, Technology Communication Tools, and Leadership Development Expectations. There are two Governor's STEM Academies (Marshall and Chantilly), which have developed cyber security camps during summer months. The Virginia General Assembly allocated grant funds for 32 cyber camps in the summer of 2016 through the Virginia Department of Education.

Seventeen of Virginia's 23 community colleges offer one or more courses aligned to cyber security, and eight offer security certificates. Three—Lord Fairfax Community College, Northern Virginia Community College, and Tidewater Community College—are designated as National Centers of Academic Excellence, with more pursuing accreditation. With the growth of new programs around the Commonwealth, the Virginia Community College System saw huge enrollments in Fall 2015 at 732 students up from 180 students in Fall 2014 (407% growth).

According to the Bureau of Labor Statistics, Virginia ranks first in the nation in the percentage of computer systems analysts and computer software

Virginia is training its workforce now.

We provide innovative cyber training to speed worker readiness for the New Virginia Economy:

Cyber Boot Camp: Cyber Education training for high school teachers and students

Conference on Cyber and Education: Discussion and education on the importance of training for cyber careers

Cyber Range: Secure platform built for training, research and collaboration

[23] http://www.doe.virginia.gov/administrators/superintendents_memos/2016/040-16a.pdf

Virginia's Commitment to Cyber Security in Higher Education

In 2016, the Commonwealth instituted two grant programs that support students seeking education and credentials in cyber security related fields. These grants bolster the current commitment to STEM fields provided by the Two Year College Transfer Grant Program.

Cyber Security Scholarship for Service

Offered through the State Council on Higher Education in Virginia, the Cyber Security Scholarship is designed to obtain commitments from students to work in state government in the field of cyber security. $500,000 has been appropriated for this program in the 2016-2017 Academic Year.

New Economy Workforce Credential Grant Fund and Program

This grant opportunity supports students as they complete high demand workforce credentials. While a list of eligible programs in currently being developed by the state Workforce Board, information technology and cyber security are both in high demand and currently emphasized.

Two-Year College Transfer Grant Program (CTG)

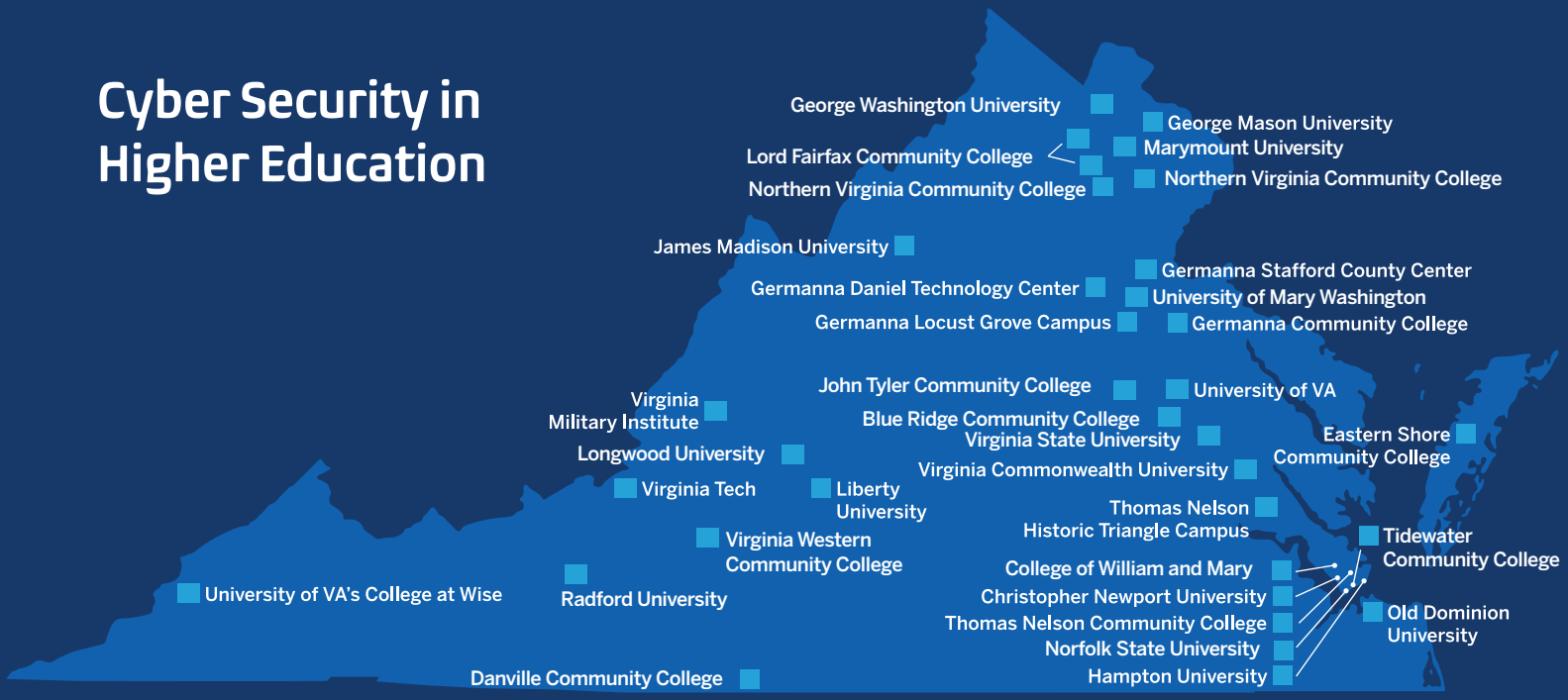
CTG qualifying students receive $1,000 per year if enrolled in STEM programs, such as information technology or cyber security degree programs.

engineers in the workforce. Every year, Virginia's universities have more than 15,000 graduate students pursuing advanced degrees in science and engineering.

As Virginia universities have contributed to preparing the workforce by offering various degrees associated with cyber security/information technology, they also support activities to enhance traditional course offerings with competitions, challenges, and student scholarship programs. For example:

- In Fall 2015, George Mason University's Volgenau School of Engineering became the first college in the nation to offer a cybersecurity engineering degree that focuses on cyber-resilience engineering design. It also runs summer camps for children and outreaches to high school students, boosting interest in the STEM fields.
- George Mason has joined a new research and training initiative of the U.S. Army Reserve (USAR), the Cyber P3i, which is a Private Public Partnership designed to enhance operational readiness in the U.S. Army. The initiative also seeks to address the national shortage of cybersecurity professionals. Mason's #7 ranking by Ponemon/HP as a top national cyber program was an important factor used by USAR to select the initial group of six universities to launch the partnership.
- Norfolk State leads a $25 million effort that begins with kindergarten activities in an effort to develop cyber security professionals. Funded by the Department of Energy, Norfolk State is leading a consortium of Historically Black Colleges and Universities, a school division, and the Department of Energy National Laboratories to develop STEM education that will lead to security careers.
- Virginia Tech, James Madison University, Marymount University, and Hampton University participate in the Federal CyberCorps Scholarship for Service program, which provides full tuition and up to $25,000 per year in scholarships to students interested in pursuing careers in cybersecurity. The program is open to students majoring in computer science or computer engineering.

Cyber Security in Higher Education



- James Madison University hosted a cyber security boot camp for high school teachers during the summer of 2015 to raise awareness and encourage the integration of cyber security topics into the curriculum.
- Virginia Tech hosted the 2015 U.S. Cyber Challenge and Cybersecurity Camp for high school students in the eastern United States. This competition seeks to recruit 10,000 of America's brightest students to usher into next generation cyber security professional jobs.

National Initiative for Cybersecurity Education

The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort to advance education and training opportunities for cyber security career preparation. NICE is coordinated by the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce. NICE defines the work within the cyber security field to help maintain a globally competitive cyber security workforce and broaden the pool of skilled workers capable of supporting a cyber-secure nation. It includes federal departments and agencies, industries, and academic institutions beginning with K-12. NICE has 13 Virginia affiliates, including seven educational institutions: *George Mason University, Hampton University, James Madison University, Marymount University, Norfolk State University, Northern Virginia Community College, and Virginia Tech*.[24]

Cyber Security Centers of Excellence

NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Information Assurance and Cyber Defense (IA/CD) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. This unique designation is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation.

Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our nation's information systems.

Virginia boasts thirteen Centers of Academic Excellence at eleven institutions.

[24]http://niccs.us-cert.gov/footer/about-national-initiative-cybersecurity-education

National Centers of Academic Excellence in Virginia

College/University	Programs offered		Honors
George Mason University Fairfax, Virginia 4 Year / Public	Masters Degree	M.S. in Information Security and Assurance	
		M.S. in Applied Information Technology with concentration in Cyber Security	
		M.S. in Computer Forensics	
		M.S. in Data Analytics with concentration in Digital Forensics	
		M.S. in Management of Secure Information Systems	
	Bachelors Degree	B.S. in Information Technology with concentration in Information Security	
		Bachelor of Applied Science with Concentration in Cyber Security	
		B.S. in Cyber Security Engineering	
	Graduate Certificate	Graduate Certificate in Applied Cyber Security	
		Graduate Certificate in Information Security and Assurance	
		Graduate Certificate in Tactical Computer Operations	
		Graduate Certificate in Telecommunications Forensics and Security	
	Center/ Institute	Mason Center for Security Information Systems	
		Center for Assured Research and Engineering	
Hampton University Hampton, Virginia 4 Year / Private	Masters Degree	M.S. for Information Assurance	Center of Academic Excellence in Information Assurance Education NSF CyberCorps Scholarship for Information Assurance recipient
James Madison University Harrisonburg, Virginia 4 Year / Public	Masters Degree	M.S. in Computer Science with concentration in Information Security and Digital Forensics	National Center of Excellence in Information Assurance Education NSF CyberCorps Scholarship for Information Assurance recipient
		M.B.A. with concentration in Information Security	
	Bachelors Degree	B.S. in Intelligence Analysis	
	Certificate	Certificate in Information Systems Security	
		Certificate in Network/Information Security	
	Professional Development	VATCyber Boot Camp and GenCyber Boot Camp instructing teachers in cyber security education	
	Partnerships/ Consortiums	Partners with Commonwealth Center for Advanced Logistics Systems	

College/University	Programs offered		Honors
Longwood University Farmville, Virginia 4 Year / Public	Minor	Minor in Cyber Security, Forensics and Policy	National Center for Digital Forensics Academic Excellence by US Department of Defense
	Partnerships/ Consortiums	Partners with Commonwealth Center for Advanced Logistics Systems	
Lord Fairfax Community College Middletown, Virginia 2 Year / Public	Career Studies Certificate	Career Studies Certificate in Cyber Security	National Center of Academic Excellence in Cyber Defense for 2 Year Education
	Associates Degree	A.A.S. in Information Systems Technology with concentration in Cybersecurity	
Marymount University Arlington, Virginia 4 Year / Private	Masters Degree	M.S. in Cybersecurity	Center for Academic Excellence in Cyber Defense NSF CyberCorps Scholarship for Information Assurance recipient
		M.S. in Information Technology with concentration in Cybersecurity	
		Dual Degree Program (M.S. in Information Technology and M.S. in Cybersecurity)	
	Bachelors Degree	B.S. in Information Technology with concentration in Networking and Cybersecurity	
	Combined Degree Program	Combined B.S./M.S. Program in Information Technology and Cybersecurity	
	Graduate Certificate	Graduate Certificate in Cybersecurity	
	Certificate	Undergraduate Certificate in Computer Networking and Cybersecurity	
Norfolk State University Norfolk, Virginia 4 Year	Masters Degree	M.S. in Computer Science with concentration in Information Assurance	Center of Excellence in Cybersecurity Research Center of Academic Excellence in Cyber Defense Education Consortium Enabling Cybersecurity Opportunities and Research Grant recipient
		M.S. in Cyber Security	
	Bachelors Degree	B.S. in Computer Science with concentration in Information Assurance	
Northern Virginia Community College Springfield, Virginia 2 Year / Public	Associates Degree	Cybersecurity AAS Degree	National Center of Academic Excellence in Information Assurance for 2 Year Education

College/University	Programs offered		Honors
Radford University Radford, Virginia 4 Year / Public	Masters Degree	M.S. in Data and Information Management with course in Security Analytics	Center for Academic Excellence in Cyber Defense
	Bachelors Degree	B.S. in Computer Science and Technology with course in core security	
		B.S. in Information Science and Systems with course in core security	
	Certificate	Certificate in Information Security	
	Course	Graduate course in cyber security education for K-12 teachers	
Tidewater Community College Norfolk, Virginia 2 Year / Public	Associates Degree	A.A.S. in Information Systems Technology with an emphasis in Cybersecurity	National Center of Academic Excellence in Information Assurance for 2 Year Education
	Career Studies Certificate	Career Studies Certificate in Cybersecurity	
Virginia Tech Blacksburg, Virginia 4 Year / Public	Minor	Minor in Cybersecurity	Intelligence Community Center for Academic Excellence NSA/DHS Center for Academic Excellence CyberCorps Scholarship for Information Assurance recipient
	Graduate Certificate	Graduate Certificate in Cyber Security	
	Laboratory	Information Technology Security Laborator	
	Center/ Institute	Security and Software Engineering Research Center	

Virginia's Cyber Security Industry

Success in developing an industry can be seen in how the companies, workforce, and products are received in the market place, and in all three indicators Virginia is leading the nation. The Commonwealth is home to more than 650 cyber security companies alone, up from 450 in 2011. These include small, medium, and large companies with a diverse array of services and clients. In addition, Virginia has 19,314 technology companies and 280,906 technology occupations. The Commonwealth is third nationally in computer systems design and related services jobs, employing 142,600; fifth in employing engineering services; and third in computing systems design and related services jobs.[25]

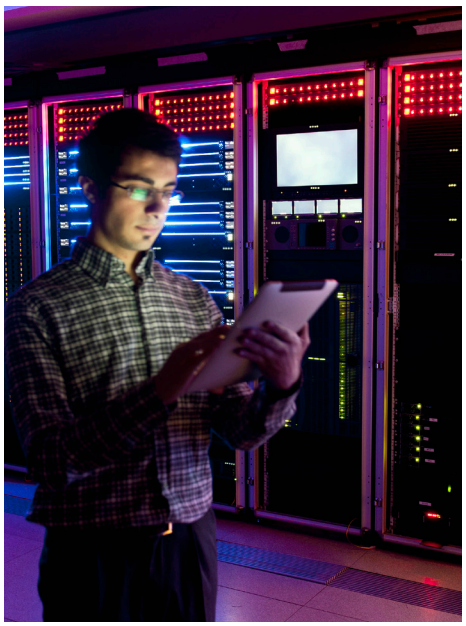
Forty of the Washington Technology Top 100 federal contracting companies are headquartered in Virginia. In the past five years, there have been more than 20 announcements related to cyber security plans to create an additional 980 jobs from companies such as Cyber Defense Solutions, FoxGuard Solutions, Telos, Kaspersky Government Security Solutions, Technology Management Solutions, and GE.[26] Demand is expected to continue to grow in this technology sector through at least 2020 with the number of persons employed in this occupational group in the Commonwealth expected to increase by 25 percent through 2022, surpassing the national expectation of just over 17 percent in that same timeframe.[27]

Virginia is also the headquarters to a number of IT Security Consulting companies such as Booz Allen Hamilton, who are all expecting to see a 68 percent rise in revenues industry-wide. Industry partners in the public and private sector are among Virginia's greatest assets in developing the strongest cyber security portfolio internationally.

Success Stories

Sera-Brynn[28]

Sera-Brynn, headquartered in Suffolk, Virginia, retained its elite standing in top the cyber security firms in the world moving up to no. 10 in the United States and continuing at no. 16 in the world rankings of like companies. Sera-Brynn approaches the cyber security



partnerships collaboratively as illustrated by CEO Rob Hegedus when he says, "Addressing cyber security requirements and response activities is more and more becoming a community-based approached." Sera-Brynn's clients include Fortune 1000 companies, healthcare, financial institutions, insurance carriers and reinsurers, higher education, municipalities and state governments, manufacturers, law offices, and more.

Verisign[29]

Verisign is a global leader in domain name and internet security and a leading provider of infrastructure services. This Reston, VA based company operates two of the internet's root servers and performs the root-zoned maintainer functions for the core of the Internet Domain Name System (DNS). Verisign ensures online businesses are available through a platform of Security Services that include intelligence-driven Distributed Denial of Service Protection, iDefense© Security Intelligence and Managed DNS. Verisign also ensures the long-term stability, security, and resilience of authoritative directoy for all .com, .tv, .cc, .name top-level, and .net domain names as well as the back-end registry for a portfolio of generic top-level domains.

Invincea[30]

With technology born out of a joint program between company founders and George Mason University's Center for Secure Information Systems, Invincea has become a leader in the protection of IT threats that impact business. More than 25,000 customers now rely on Invincea to prevent and detect threats and to enable their workforce in diverse climates. Invincea is now ranked in the top 500 Cybersecurity firms in the world.

AxonAI[31]

Axon AI is a leading cyber security firm focused on the Internet of Things (IoT) developing across and throughout technology industries. By providing a three product approach that address massive parallel, autonomous processes, scales to working with any database size, and capable of utilizing swarming technologies, AxonAI is positioning itself as a leader in the IoT space to collaborate with such innovative manufacturers as SAP, Amazon Web Sevices, NVIDIA, and Google.

L-3 & Northrop Grumman

Both L-3 Communications and Northrop Grumman offer a diverse, compelling platform of cyber security products and

[25]CompTIA LLC, 2015
[26]http://www.yesvirginia.org/Content/pdf/Industry%20Profiles/VA%20Cybersecurity%20Summary%202016.pdf
[27]Idib Pg 4
[28]https://sera-brynn.com/sera-brynn-moves-top-10-u-s-cybersecurity-500-top-global-cybersecurity-firms
[29]http://cybersecurityventures.com/cybersecurity-500/#home/viewdetails/54ce2314ae73104b48470e8c/
[30]https://www.invincea.com
[31]http://axonai.com/our-work

platforms and are both based in Virginia. Ranked 54 and 55 in the top cyber security firms in the world, federal, state, and private entities are able to incorporate world-leading technologies easily.

ThreatQuotient

Founded in 2013, Sterling, VA-based ThreatQuotient was awarded as the silver "Security Start Up of the Year" at the 2016 Info Security Global Excellence Awards, part of the RSA Conference. ThreatQuotient received funding through the Virginia Center for Innovative Technology GAP Fund, and offers ThreatQ, a threat intelligence platform that centrally manages and correlates external sources with internal security and analytics solutions for contextual and operationalized intelligence. The company's platform has integrations with commercial intelligence feeds, OSINT feeds, private feeds, import threat intelligence via email, and advanced threat solutions/malware sandboxes.

Companies Listed in the Top 500 Cybersecurity Companies in the World located in Virginia

Company	Cybersecurity Sector	Corporate HQ
Sera-Brynn	Cyber Risk Management	Suffolk, VA
IKANOW	Information Security Analytics	Reston, VA
VeriSign	Internet Security Solutions	Reston, VA
Northrop Grumman	Cyber & Homeland Security Services	McLean, VA
L-3	National Security Solutions	Reston, VA
Novetta	Cyber Security Analytics	McLean, VA
Leidos	Anti-Terrorism & Homeland Security	Reston, VA
CYREN	Web, Email & Mobile Security	McLean, VA
CyFIR	Digital Forensics & e-Discovery	Manassas, VA
Haystax	Advanced Threat Analytics	McLean, VA
LookingGlass	Cyber Threat Intelligence Management	Arlington, VA
SAIC	Cybersecurity Professional Services	McLean, VA
Siemens Government Technologies	Cybersecurity for Federal Government	Arlington, VA
ThreatQuotient	Threat Intelligence Platform	Reston, VA
MeasuredRisk	Cyber Advisory & Risk Analysis	Arlington, VA
Centripetal	Cyber Threat Intelligence	Herndon, VA
Paraben	Digital Forensics & Data Recovery	Ashburn, VA
MindPoint Group	IT Security Solutions	Springfield, VA
Ntrepid	Secure Network & Online Computing	Herndon, VA
Oberthur Technologies	Digital Security for Mobility	Chantilly, VA
CACI	Intelligence, Defense & Federal Security	Ballston, VA
General Dynamics	IT Cybersecurity Solutions	Fairfax, VA
PhishMe	Phishing Attack Defense	Leesburg, VA
MicroStrategy	Mobile Identity Platform	Tysons Corner, VA

Company	Cybersecurity Sector	Corporate HQ
Daon	Identity Assurance & Biometrics	Fairfax, VA
PFP Cybersecurity	IoT Security	Vienna, VA
Defense Point Security	Cybersecurity Services for Federal Agencies	Alexandria, VA
CSC	IT Security Services	Falls Church, VA
Invincea	Malware Detection & Prevention	Fairfax, VA
Endgame	Security Intelligence & Analytics	Arlington, VA
ePlus Security	Infosecurity Services & Products	Herndon, VA
Verodin	Cyber Attack Simulations	Reston, VA
AxonAI	Internet of Things Security	Harrisonburg, VA
Cigital	Application Security Testing	Dulles, VA
ThreatConnect	Cyber Threat Intelligence Platform	Arlington, VA
GuidePoint Security	Information Security Services	Reston, VA
Risk Based Security	Cyber Risk Analytics	Richmond, VA
SurfWatch Labs	Cyber Risk Intelligence Analytics	Sterling, VA
Distil Networks	Malicious Bot Detection & Prevention	Arlington, VA
Veris Group	Cybersecurity Professional Services	Vienna, VA

The Federal Connection: Federal Cyber Security Investments and Initiatives

Proximity to Decision-Makers

Virginia exhibits unique qualities that most other states cannot claim. Its geographical location allows for companies to have access to the nation's political decision-making center in Washington, D.C. With unparalleled access to federal legislators and the executive branch, educational and business groups have seen it in their own best interests to call Virginia home. Federal contract spending in Virginia increased nearly $1 billion in 2014 over 2013, the most out of all 50 states.[32] Deltek forecasts the demand for vendor-furnished information security products and services by the U.S. federal government will increase from $8.6 billion in FY 2015 to $11.0 billion in 2020 at a compound annual growth rate (CAGR) of 5.2 percent.[33]

Virginia is home to several federal agencies that focus on cyber security and offer contract relationships to the industry including the U.S. Army Cyber Command (ARCYBER), U.S. Department of Defense, U.S. Department of Homeland Security's National Cyber Security and Communications Integration Center, and the Defense Advanced Research projects Agency (DARPA).[34] Educational partners such as the International Cyber Center (ICC) at George Mason University, The Center for Secure Information Systems (CSIS), Cyber@VT and the Hume Center for National Security and Technology, The Cybersecurity Innovations Laboratory,

Federally Funded Research Centers in Virginia

Facility	Location
National Security Engineering Center	Bedford, MA McLean, VA
Center for Advanced Aviation System Development	McLean, VA
Center for Enterprise Modernization	McLean, VA
National Security Engineering Center	Bedford, MA McLean, VA
Center for Advanced Aviation System Development	McLean, VA
Center for Enterprise Modernization	McLean, VA
Centers for Communications and Computing	Alexandria, VA
CMS Alliance to Modernize Healthcare	McLean, VA
Homeland Security Studies and Analysis Institute	Arlington, VA
Homeland Security Systems Engineering and Development Institute	McLean, VA
Judiciary Engineering and Modernization Center	McLean, VA
National Radio Astronomy Observatory	Charlottesville, VA
Studies and Analyses Center	Alexandria, VA
Thomas Jefferson National Accelerator Facility	Newport News, VA

Federal Entity Offices in Virginia

Facility	Location
Langley Research Center (LaRC)	Hampton, VA
Wallops Flight Facility	Wallops Island, VA
Thomas Jefferson National Accelerator	Newport News, VA
United States Patent and Trademark Office (PTO)	Alexandria, VA
National Cybersecurity & Communications Integration Center	Arlington, VA
Air Force Office of Scientific Research (AFOSR)	Arlington, VA
National Science Foundation (NSF)	Arlington, VA
Office of Naval Research (ONR)	Arlington, VA
United States Fish & Wildlife Service	Falls Church, VA
Foreign Service Institute	Arlington, VA
Nuclear Waste Technical Review Board	Arlington, VA
US Marshals Service	Arlington, VA
Army National Guard Readiness Center	Arlington, VA
Joint Improvised Explosive Device Defeat Organization	Arlington , VA
United States Air Force (USAF)	Arlington , VA

[32]National Contract Management Assiciation (NCMA), Bloomberg Government, Annual Review of Government Contracting 2015 edition,
[33]Government Research Reports, Federal Information Security Market, 2015-2020 (Oct 2015)
[34]Idib Pg 6

Photo by NASA HQ PHOTO

and James Madison University's Institute for Infrastructure and Information Assurance (IIIA) interface directly with these agencies; providing mechanisms and opportunities for professionals, educators, and students to engage with federal agencies and private companies like L-3 Communications and Amazon Web Services. Engagement across industries, governments, and markets is the fundamental key to the Commonwealth's leadership success and provides a unique framework for success recognized as a national leader.

NASA & The Defense Industry

The National Aeronautics and Space Administration (NASA) and the defense industry as a whole should not be overlooked as a unique provider of opportunity in Virginia. While the defense industry is spread throughout the nation, Virginia's position is unique in the breadth of contracts and relationships available through the Department of Defense (DoD).

As of FY 2013, Virginia accounted for more than $44.6 billion in defense contracts alone, making it the No. 1 state for total revenue driven by DoD investment.[35] This success is not driven simply by the geographical access to Washington D.C., but is driven by the long-term investments made by leading companies and government agencies in the region; an investment that is likely to continue growing with the business friendly environment and partnership development in cyber security.

Twelve defense contractors are headquartered in Virginia, including Alliant Techsystems, Atlantic Diving Supply, Booz Allen Hamilton, CACI, CSC, DynCorp, General Dynamics, Huntington Ingalls, ITT Exelis, Leidos, ManTech, and Northrop Grumman. While such heavy-hitters in the same field may intimidate some companies, by being co-located in the Virginia area, new companies gain access to corporate entrepreneurial initiatives that enable cross-collaboration, increased likelihood of buyout, and a "Silicon Valley" like atmosphere focused in their field.

These defense contractors have seen the value in access to national leaders in Washington D.C., as well as a close proximity to the Pentagon and nineteen defense installations. With the Federal government focusing on investing in start-up companies by making access to venture capital easier for government related tech firms, localizing a business in Virginia has never been more important.[36]

These nineteen defense installations have cultivated programs that enable service members and procurement officers to engage with communities in the industry. By collaborating locally, diminishing the need for travel expense and increasing face-to-face communication and discussion, cyber security companies gain a leg up on any non-local competition. These Defense installations, defense contractors, and smaller firms have therefore been able

[35]Say Yes to Aerospace in Virginia, Yestovirginia.org.

to create collaborative partnerships and projects much easier than with other organizations; leading directly to research and development capabilities throughout the state.

Research and development is the first fundamental step toward innovation. By collaborating with competitors and developing private-partnerships that enable potential customers to outline their needs directly to engineering production, the iterative process of innovation comes faster and with much greater return. Virginia has therefore made these partnerships its main focus over the last five-years, and the area is reaping the rewards of those efforts.

Virginia now boasts significant partnerships between NASA, DoD, and private companies. The Virginia Modeling and Simulation Center (VMASC) applies simulation techniques to solve problems and provides training for industry, military and governments. Virginia's unique partnerships also include the Defense Advanced Research Projects Agency (DARPA) that enables private companies and universities to respond to military proposals and start-up oriented engineering labs all over the country.

Virginia as a Connector

Virginia is unparalleled in helping private companies interface and develop cross-industry relationships with military and federal government entities through its proximity to the nation's capital, and to the Virginia-based Federally Funded Research and Development Centers (FFRDC) such as MITRE and the Aerospace Corporation; research consortiums such as The Commonwealth Center for Advanced Manufacturing (CCAM) and the Commonwealth Center for Advanced Logistics Systems (CCALS); government research organizations such as the National Aeronautics and Space Administration (NASA); and the Virginia Cyber Security Partnership. By addressing a variety of industries and involving private and public entities, Virginia's ecosystem of innovation is driving the frontier of cyber security technologies as no other state can.

The Commonwealth of Virginia recognizes its role as the partnering force between the federal government and private industry to accomplish the vital task of supporting American interests throughout the world and to provide the workforce, education, infrastructure, and pro-business environment to help those partnerships flourish. The federal government, led by the February 2016 initiative to invest over $19 billion for cyber security as part of the President's Fiscal Year (FY) 2017 Budget – a 35 percent increase from FY 2016 – represents the continued growth in support and need.[37]

[36]https://www.whitehouse.gov/startup-america-fact-sheet
[37]https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

More recently, a **Cybersecurity National Action Plan (CNAP)**, and an additional $3.1 billion to modernized, retire, or replace outdated IT infrastructure characterizes the federal support for cyber security issues. The CNAP also routes an additional **$62 million for cyber security personnel**, especially those at the National Centers for Academic Excellence Cybersecurity Program locations including George Mason University, Hampton University, James Madison University, Lord Fairfax Community College, Marymount University, Norfolk University, Northern Virginia Community College, Radford University, Tidewater Community College, and Virginia Polytechnic Institute and State University – all located in the Commonwealth of Virginia.[38]

Beyond those institutions within Virginia that are heavily involved with the federal government already, Virginia seeks to be a home for new developing technology partnerships such as the newly envisioned **Cybersecurity Assurance Program**, **National Center for Cybersecurity Resilience**, and to be a leading voice in the public-private partnerships between technology companies and government envisioned by the White House in February 2016.[39] The federal government has signaled their long-term interest in partnering with states that are pro-business, locally accessible to help reduce logistical costs, and able to meet the current and future challenges facing the country. Private industry has also shown interest in investing in cyber security technologies, estimating a market size of $77 billion in 2015 with growth to $170 billion by 2020 with active participation by venture capital and new accelerator program development through Virginia.[40]

The Commonwealth of Virginia is considered the top recipient of federal contracts as a result of unique resources that will not change moving forward, including proximity to Washington, D.C., being home to the Pentagon, Quantico, and other Federal Agency Headquarters, and providing a very pro-business financial structure.[41] The Northern Virginia area, specifically, is in considered to be in the "best position in the nation to be the next "Silicon Valley" of cyber security as it combines a "developing workforce ...

[38]https://www.iad.gov/NIETP/reports/current_cae_designated_institutions.cfm
[39]https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf
[40]http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#1ff1b58710b2
[41]National Contract Management Association. Annual Review of Government Contracting, 2015 Edition. Pg. 7

advanced and modern infrastructure ... and proximity to end-users."[42]

It will take true leadership, partnership, and support from government to meet the new challenges brought on by technologies cultivated today and Virginia is set to set the benchmark for innovative solutions. IoT is expected to bring on new challenges and "lift cyber security spending and research through 2025 ... while a cyber security workforce shortage is expected to reach 1.5 million unfilled positions by 2019."[43] Virginia is ahead of the game; addressing both needs through the creation of industry led accelerator programs, academic and private research oriented collaborations, and heavy investment in the public university system cultivating tomorrow's leaders, today. Virginia's Centers of Excellence for Education in Cyber Security, Centers of Excellence for Research in Cyber Security, and Scholarship for Service where cyber security students earn federal financial assistance are sterling demonstrations of Virginia's leadership in education solving the needs of industry.[44]

Cyber Security: Another Important Piece of the Innovation Ecosystem

The Commonwealth does not see cyber security as a technology industry that stands alone, but instead sees it as another important partner in the innovative landscape for the future that the governor's office has worked diligently to cultivate. Virginia is now a world leader in the field of Unmanned System Technologies (UMS) throughout ground, air, sea and space and leads the nation as one of only 6 FAA designated test-sites in the United States – the Mid-Atlantic Aviation Partnership (MAAP). MAAP's Virginia lead is the Secretary of Technology Karen Jackson who also co-chaired the Virginia Cyber Security Commission which outlined the states policies and goals for cyber security initiatives and needs.

Both industries have similar problems and needs, and with leadership involved in both initiatives private companies have a knowledgeable and involved executive with whom to align their own expectations. The UMS industry considers cyber security one of the most important elements in enabling future developments and integration into commercial operations. The FAA, AUVSI, and other stakeholders all cite communications protection, data and privacy security, and signal assurance as necessary to success in unmanned robotics. These technologies must grow together, and industry relationships developed in Virginia will enable that growth with significant efficiency and effectiveness. The latest news in the Unmanned Aircraft Systems (UAS) field is the final regulations passed by the FAA which will make it much easier for commercial UAS operations to succeed. By supporting these UMS industries with regional innovation and application of cyber security, Virginia pushes the limit for where both technology industries can go.

Virginia as a Partner

The Commonwealth Research Commercialization Fund and the Center for Innovative Technologies (CIT) are key players in promoting homegrown innovation for any investment opportunities. This center, developed as a flagship for the New Virginia Economic Development Plan, thrives in the recognition that the availability of early-stage capital is a critical need of many emerging technology companies and that making connection with private, public, and international funding is a difficult step in the start-up lifecycle.[45]

CIT has created for any early-stage startup the Commonwealth Innovation and Entrepreneurship Measurement Systems (IEMS); a web-based portal using key metrics to track the performance of Virginia's innovation economy, allowing angel investors and private equity firms and other stakeholders a unique insight into the life-cycles and stages of start-up companies in Virginia along with opportunities to get involved very easily. This reduces the hurdles of engagement for investment for companies and investors alike.[46]

Small businesses have been rewarded significantly by beginning their journey in Virginia. The Small Business Innovation Research (SBIR) program and the Small Business Technology Transfer program (STTR) offer similar incentives for small business that partner with non-profit U.S. research institutions. Virginia based firms, because of the local and supported access to non-profit organizations such as universities, military and non-military government groups, and R&D laboratories received a total of $109.6 million in SBIR/SBTT funds in 2014; the third highest amount of any state. [47]

By focusing on all levels of a company's life cycle, Virginia provides the perfect environment to start, grow, and commercialize any cyber-related firm. By taking advantage of the unique characteristics and government support provided in Virginia, companies make a smart decision for their future. ■

[42]http://passcode.csmonitor.com/goldrush
[43]http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/3/#15e47bfb26f9
[44]https://cyberva.virginia.gov/media/4396/cyber-commission-report-final.pdf
[45]http://www.cit.org/service-lines/cit-entrepreneur
[46]http://www.cit.org/initiatives/iems/measurement-system/
[47]http://www.cit.org/initiatives/iems/research-and-development/

Incentives

New Virginian companies can be supported by a number of unique incentives geared toward enabling technologies in sub-markets. While this has created a friendly environment for all business development within the state for new or expanding firms, there are number of technology focused programs of which to be aware.

Commonwealth's Opportunity Fund

The Commonwealth's Opportunity Fund (COF) is a discretionary incentive available to secure a business location or expansion project for Virginia. Grants are awarded to localities on a local-matching basis with the expectation that the grant will result in a favorable location decision for the Commonwealth.

Grant requests are made by the community for a project under the following conditions:

- Projects must meet investment, job creation, and wage minimums
- Matching local financial participation is required on a dollar-for-dollar basis (cash or in-kind)
- Public announcement of the project must be coordinated by the Virginia Economic Development Partnership and the Governor's Office (neither the company nor the locality may publicly confirm the proposed project)
- Grants are made at the discretion of the Governor

http://www.yesvirginia.org/ProBusiness/BusinessIncentives

Governor's Development Opportunity Fund

The Governor's Development Opportunity Fund (GOF) provides either grants or loans to localities to assist in the creation of new jobs and capital investment in accordance with criteria established by legislation.

General Eligibility Thresholds:

- 50 new jobs / $5 million capital investment; or
- 25 new jobs / $100 million capital investment

The average annual wage for the new jobs must be at least equal to the prevailing average annual wage in the locality, excluding fringe benefits. If the average annual wage is twice the prevailing average annual wage, the Governor may reduce the new jobs threshold to as low as 25

http://www.virginiaallies.org/assets/files/incentives/GOFGuidelines.pdf

Virginia Investment Partnership Act/Major Eligible Employer Grant

The Virginia Investment Partnership (VIP) Grant and the Major Eligible Employer Grant (MEE) are designed to encourage continued capital investment by Virginia companies. This is intended to add capacity, modernize, increase productivity, creation, development, and utilization of advanced technology. UMS technologies are specifically being targeted for this type of investment.

To be eligible for a VIP grant, a minimum of $25 million in capital investment is required by an eligible existing Virginia manufacturer or research and development service.

http://www.virginiaallies.org/assets/files/incentives/VIPGuidelines.pdf

The Virginia Economic Development Incentive Grant

The Virginia Economic Development Incentive Grant Program (VEDIG) assists and encourages companies to invest and to provide new employment opportunities by locating significant headquarters, administrative, research and development, and/or similar service and basic sector operations in Virginia. This is a discretionary program in which grants are negotiated and offered to qualified applicants as an economic development incentive.

The VEDIG program has two separate eligibility requirements. Companies located in a Metropolitan Statistical Area with a population of 300,000 or more in the most recently preceding decennial census, must:

- Create or cause to be created and maintained (i) at least 400 jobs with average salaries at least 50% greater than the prevailing average wage; or (ii) at least 300 jobs with average salaries at least 100% greater than the prevailing average wage
- Make a capital investment of at least $5 million or $6,500 per job, whichever is greater. For all companies located elsewhere in Virginia, the company must create or cause to be created and maintained at least 200 jobs with average salaries at least 50% greater than the prevailing average wage, and make a capital investment of at least $6,500 per job

http://www.virginiaallies.org/ assets/files/ incentives/VEDIGGuidelines.pdf

Tobacco Region Opportunity Fund

The Tobacco Region Opportunity Fund is available to tobacco producing regions to assist with specific projects that result in the crea-tion of new jobs and investment. Grants are made to the community at the discretion of the Tobacco Region Revitalization Commission. The goal of the fund is to attract competitive projects ex-pected to have a regional impact due to the magnitude of new employment and investment, and the possibility of follow-on industry.

- Evaluation of award amount is consistent throughout the region and is based on the following criteria: local unemployment rates, prevailing wage rates, number of new jobs, capital investment levels, industry type, and the possibility of related economic multiplier effect
- TROF is the only Tobacco Commission grant program paid at the beginning of the project to help tobacco region localities be competitive in attracting new investment and jobs resulting in increased tax revenue and opportunity for quality employment in the tobacco region
- Intended to support the goal of the Commission to "revitalize the economies of tobacco-dependent regions and communities." This goal is measured by job creation, workforce participation rate, wealth, diversity of economy, and taxable assets. All measurements listed are increased when a new or expanding business in the tobacco region creates new jobs that pay more than prevailing wage and adds taxable assets to the local tax rolls

http://www.tic.virginia.gov/tobregionoppfund.shtml

Center for Innovative Technology Incentives

Commonwealth Research Commercialization Fund

The Commonwealth Research Commercialization Fund (CRCF) accelerates innovation and economic growth in Virginia by advancing solutions to important state, national, and international problems through technology research, development, and commercialization. Cyber security has been identified as a critical field of study.

Proposals submitted to CRCF undergo a multi-stage review process, which includes award recommendations made by the Research and Technology Investment Advisory Committee (RTIAC) to the CIT Board of Directors and culminates with award decisions made by the Board. CRCF awards contribute to the Commonwealth's overall plan to enhance economic development through technology research and commercialization and, as such, CRCF awards must further the goals set forth in the Commonwealth Research and Technology Strategic Roadmap. In addition to identifying research areas worthy of economic development and institutional focus, the Roadmap provides a framework for aligning key industry sectors within the state, as prioritized by the research community, which includes but is not limited to the private sector, academia, and economic development professionals.

http://www.cit.org/initiatives/crcf/

CIT GAP Funds

CIT GAP Funds is a family of seed-and early-stage investment funds placing near-equity and equity investments in Virginia- based technology, life science, and clean tech companies. CIT GAP Funds invests in companies with a high potential for achieving rapid growth and generating significant economic return for entrepreneurs, co-investors and the Common-wealth of Virginia.

CIT's family of funds includes:

- GAP Fund I – A vintage 2004 fund fully invested in a broad array of seed-stage technology companies
- GAP BioLife Fund – A seed fund investing exclusively in life science companies
- GAP Tech Fund – A seed fund investing in IT and technology companies
- Commonwealth Energy Fund (CEF), a seed fund investing in energy efficiency and renewable energy companies

http://www.cit.org/service-lines/cit-gap-funds/

CIT GAP Tech Fund

The CIT GAP Tech Fund makes seed-stage equity investments in Virginia-based technology companies with a high potential for achieving rapid growth and generating significant economic return. The fund invests exclusively in companies headquartered, and with an express desire to grow in the Commonwealth of Virginia.

Sectors (includes cyber security)

- Software, Telecommunications
- Semiconductors
- Security
- Information and Communication

Technologies

- E-Commerce
- Networking and Equipment
- Electronics/Instrumentation
- Computers and Peripherals
- Sensors
- Materials

http://www.cit.org/service-lines/gap-tech-fund/

Business Development Tax Credits

Refundable Research and Development Expenses Tax Credit

This credit is an individual and corporate income tax credit for certain taxpayers that incur Virginia qualified research and development expenses.

During the 2014 Session, the Virginia General Assembly enacted legislation that increased the overall credit cap, increased the per taxpayer credit cap, allows pass-through entities to elect to claim the credit at the entity level, and requires taxpayers to provide certain information to the Department of Taxation ("the Department") when applying for the credit

http://www.tax.virginia.gov/content/rd

Enterprise Zone Tax Credit

This credit provides state and local incentives to businesses that invest and create jobs within Virginia's enterprise zones, which are located throughout the state.

http://www.tax.virginia.gov/content/tax-credits#enterprise

Major Business Facility Job Tax Credit

Through this credit qualified companies locating or expanding in Virginia receive a $1,000 income tax credit for each new full-time job created over a threshold number of jobs.

- Companies locating in Enterprise Zones or economically distressed areas are required to meet a 25-job threshold; all other locations have a 50-job threshold. The threshold number of jobs must be created within a 12-month period
- The $1,000 credit is available for all qualifying jobs in excess of the threshold and is taken in equal installments over two years ($500 per year) through 2014. Credits earned after 2014 will be taken in equal installments over three years
- Non-qualifying jobs include seasonal positions shifted within Virginia, building and grounds maintenance, security, and other positions ancillary to the principle activities of the facility
- Credits are available for taxable years before January 1, 2020. Unused credits may be carried over for up to 10 years

http://www.tax.virginia.gov/content/tax-credits#Major_Business_Facility_Job_Credit

Qualified Equity And Subordinated Debt Investments Credit

This credit offers angel investors a 50% tax credit for pre-qualified small business ventures involved in technology fields. The state also offers individual and corporate income tax subtractions for long-term capital gains attributable to qualified investments in early stage technology, biotechnology, and energy start-ups; technology, nanotechnology, or any similar technology-related field, which includes cyber security.

- The credit is equal to 50% of the qualified business investments made during the taxable year. If total annual requests for the credit exceed $5 million for tax year 2015, the Department of Taxation will prorate the credit for each taxpayer
- The credit a taxpayer may claim per taxable year may not exceed the credit authorized by the Department of Taxation, $50,000, or the income tax liability on that year's return, whichever is less. The credit is nonrefundable. Unused credits may be carried forward up to 15 years

http://www.tax.virginia.gov/content/tax-credits#Qualified_Equity_And_Subordinated_Debt_Investments_Credit

Telework Expenses Tax Credit

This credit allows a tax credit to employers for eligible expenses incurred for allowing employees to telework pursuant to a signed telework agreement for taxable years beginning on or after January 1, 2012, but before January 1, 2017. An employer may be eligible for a credit of up to $1,200 per teleworking employee and/or a maximum of $20,000 for conducting a telework assessment.

- The telework assessment can only be allowed once. The aggregate amount of tax credits that will be issued is capped at $1 million annually
- An employer shall be ineligible for a tax credit pursuant to this section if such employer claims a credit based on the jobs, wages, or other expenses for the same employee under any other provision of this chapter. Additionally employers are not allowed to deduct expenses that are deducted for federal purposes

http://www.tax.virginia.gov/content/tax-credits#TeleworkExpensesTaxCredit

Worker Retraining Tax Credit

This credit allows an employer to claim a tax credit for the training costs of providing eligible worker retraining to qualified employees for taxable years beginning on or after January 1, 1999. The credit may be applied against individual income tax, estate and trust tax, corporate income tax, bank franchise tax, and taxes imposed on insurance companies and utility companies.

Eligible worker retraining includes noncredit courses approved by the Virginia Economic Development Partnership. For information on noncredit course approval, call (804) 545-5706. It also includes credit or non-credit retraining courses undertaken through an apprenticeship agreement approved by the Commissioner of Labor and Industry.

The credit is generally 30% of all classroom training costs:

- Limited to up to $200 annual credit per student if the course work is incurred at a private school or $300 per qualified employee with retraining in a STEM or STEAM discipline
- The Department of Taxation is authorized to issue up to $2,500,000 of retraining credits annually. If total requested credits exceed this amount, the Department of Taxation will prorate the authorized credits
- Credits taken may not exceed tax liability in any one taxable year. Unused credits may be carried forward for three years

http://www.tax.virginia.gov/content/tax-credits#Worker_Retraining_Credit

Additional Tax Credits

Sales and Use Tax Exemption

This exemption is for purchases used exclusively in research and development.

Research and Development Tax Credit

Businesses may claim a tax credit equal to 15% of the first $234,000 in Virginia qualified research and development expenses incurred during the taxable year or they may claim a tax credit equal to 20% of the first $234,000 in Virginia qualified research and development expenses if the qualified research was conducted in conjunction with a Virginia college or university.

- $6 million cap on the total amount of credits allowed in any fiscal year

http://www.tax.virginia.gov/content/tax-credits#ResearchandDevelopmentTaxCredit

Credit for Tax Paid to Another State

The Code of Virginia makes out-of-state tax credit provisions for income taxed by more than one state. The credit is restricted to certain types of income. The intent of the law is to address double taxation when income is generated in more than one state; however, the credit does not eliminate double taxation in all cases. For example, taxes paid to another state on non-qualifying income would not be subject to the credit provisions.

Generally, Virginia will allow taxpayers filing resident individual income tax returns to claim credit for income tax paid to another state on qualifying income derived from sources outside of Virginia, provided the income is taxed by Virginia as well as the other state. If the income is from one or more of the following states, the credit should be claimed on the nonresident income tax return of the other state instead of the Virginia return: Arizona, California, District of Columbia, Oregon

http://www.tax.virginia.gov/content/tax-credits#Credit_for_Tax_Paid_to_Another_State

Programs

SSBCI Virginia Capital Access Program

This program provides loan loss insurance to a bank to cover a portfolio of enrolled loans. It is designed to be a quick, efficient means of obtaining a credit enhancement from the VSBFA. Under most circumstances, the bank determines whether a loan will be enrolled in the program without VSBFA's involvement.

- Program is designed to assist financial institutions in making small business loans by mitigating some of the risk associated with the loan
- Program offers lenders a flexible, non-bureaucratic tool to expand their market base and enhance their ability to meet the financing needs of Virginia's businesses

http://www.vabankers.org/ssbci-virginia-capital-access-program

Small Business Microloan Program

This is a direct loan from the VSBFA to the business client that does not require a bank's participation in the transaction. It is an ideal tool for bankers who are faced with business loan requests for very small amounts where the bank would prefer to refer the client to an alternative source of funds.

The Virginia Small Business Financing Authority (VSBFA) is the Commonwealth of Virginia's economic development and business financing arm and helps banks make loans to businesses that can demonstrate repayment ability, but where the bank needs additional collateral support or a more robust secondary repayment source by providing:

- Cash collateral
- Subordinate companion loans
- Guaranties
- Loan loss reserves

http://www.vabankers.org/VSBFA

Economic Development Access Program

Administered by the Virginia Department of Transportation, this program assists localities in providing adequate road access to new and expanding basic employers.

- Funds may be used for financing the construction or improvement of secondary or local system roads within all counties and cities, and certain towns that are part of the Urban System, hereinafter referred to as eligible localities
- Ancillary improvements, such as turn lanes or intersection modifications may also be warranted as part of the access project, but are not considered the primary objective of the project

http://www.virginiadot.org/business/resources/local_assistance/access_programs/EconomicDevelopmentAccessProgramGuide.pdf

Zones

Enterprise Zones

The Virginia Enterprise Zone (VEZ) program is a partnership between state and local government that encourages job creation and private investment. VEZ accomplishes this by designating Enterprise Zones throughout the state and providing two grant-based incentives, the Job Creation Grant (JCG) and the Real Property Investment Grant (RPIG), to qualified investors and job creators within those zones, while the locality provides local incentives.

State incentives are available to businesses and zone investors who create jobs and invest in real property within the boundaries of enterprise zones.

http://www.dhcd.virginia.gov/index.php/community-partnerships-dhcd/downtown-revitalization/enterprise-zone.html

Enterprise Zone Job Creation Grant

Job Creation Grants are based on net new permanent full-time job creation exceeding a four-job threshold. Positions over the four-job threshold must meet wage and health benefits requirements to be eligible for the JCG. Firms can receive grants for up to 350 positions per year.

- Business firm must be located in a Virginia Enterprise Zone
- Business firm must create at least 4 net new permanent full-time positions over the base calendar year
- Net new permanent full-time positions created over the 4-job threshold must meet wage (at least 175% of the Federal Minimum Wage, 150% in High Unemployment Areas) and health benefits requirement (at least 50% of employee's premium paid for by employer)
- Grants are available for a five-consecutive-year qualification period
- To be eligible for the JCG in years 2-5 of the grant cycle, a business firm must maintain or increase the number of eligible permanent full-time positions (above the 4-job threshold) over base year employment. Base year employment levels are established during the first grant year and will remain consistent throughout the 5-year grant period
- Firms can continue to receive grants for any net new permanent full-time positions created over base year employment levels that meet wage and health benefits requirements
- Firms may apply for a subsequent 5-year period given they meet the grant eligibility requirements. Grant Year 2011 was the first year firms were eligible to begin subsequent five-year periods

http://www.dhcd.virginia.gov/images/VEZ/JCG-Instruction-Manual.pdf

Enterprise Zone Real Property Investment Grant

Real Property Investment Grants are available for investments made to industrial, commercial, or mixed use properties located within the boundaries of Enterprise Zones. Grants are available to qualified zone investors in amounts up to 20% of the qualified real property investment, not to exceed $200,000 per building or facility within a five year period.

The property (building or facility) must be located within the boundaries of a Virginia Enterprise Zone:

- The building or facility must be commercial, industrial, or mixed-use. Mixed-use is defined as a building incorporating residential uses in which a minimum of 30% of the useable floor space is devoted to commercial, office, or industrial use
- For the rehabilitation or expansion of an existing structure, the zone investor must spend at least $100,000 in qualified real property investments to be eligible
- For new construction projects, the zone investor must spend at least $500,000 in qualified real property investments to be eligible
- Grants may not exceed $200,000 per building or facility in a 5 consecutive-year period. 5-year periods being with the qualification year in which a grant was first awarded
- After the conclusion of a 5-consecutive-year period, the property beings another eligibility period and the grant cap of $200,000 is restored

http://www.dhcd.virginia.gov/images/VEZ/RPIG-Instruction-Manual.pdf

Technology Zones

Virginia authorizes its communities to establish technology zones to encourage growth in targeted industries. Presently, 30 cities and counties and 6 towns have created zones throughout the state. Qualified businesses locating or expanding operations in a zone may receive local permit and user fee waivers, local tax incentives, special zoning treatment, or exemption from ordinances. Once a local technology zone has been established, incentives may be provided for up to 10 years.

Localities that have established technology zones include the counties of Amherst, Arlington, Bedford, Caroline, Chesterfield, Culpeper, Fauquier, Frederick, Halifax, Henry, Page, Roanoke, Rockingham, Russell, Smyth, Spotsylvania, Stafford and Warren; the cities of Buena Vista, Charlottesville, Chesapeake, Falls Church, Franklin, Fredericksburg, Harrisonburg, Lynchburg, Manassas, Manassas Park, Newport News, Poquoson, Suffolk and Winchester; and the towns of Ashland in Hanover County, Bridgewater in Rockingham County; Cape Charles in Northampton County, Front Royal in Warren County, Kilmarnock in Lancaster County, Marion in Smyth County and Wytheville in Wythe County.

http://www.virginiaallies.org/assets/files/incentives/techzonewriteup.pdf

Foreign Trade Zones

Foreign Trade Zones (FTZ) are areas which are geographically inside the United States, but are legally considered outside its Customs territory. Companies that locate in FTZs can benefit by using special procedures to encourage U.S. activity by reducing, eliminating, or delaying duties.

- Virginia offers 6 foreign trade zones designed to encourage businesses to participate in international trade by effectively eliminating or reducing customs duties
- Numerous subzones are provided and additional ones can be designated to enhance the trade capabilities of specific companies and technologies such as UMS

http://www.yesvirginia.org/ProBusiness/BusinessIncentives

Defense Production Zones

Virginia's cities, counties, and towns have the ability to establish, by ordinance, one or more defense production zones to attract growth in targeted industries. Establishment of a defense production zone allows localities to create special incentives and certain regulatory flexibility for qualified businesses locating or expanding operations in a zone. These incentives may include: reduction of user and permit fees, special zoning treatment, exemption from local ordinances or other incentives adopted by ordinance. Virginia authorizes its communities to establish local defense production zones to benefit businesses engaged in the design, development, or production of materials, components, or equipment required to meet the needs of national defense. Companies deemed ancillary to or in support of the aforementioned categories would also apply.

- Once a defense production zone is established, incentives may be provided for up to 20 years
- Each locality designs and administers its own program
- Establishment of a defense production zone shall not preclude the area from also being designated as an enterprise zone
- Two localities currently have an established Defense Production Zone:
  - Fauquier County and the City of Manassas Park;
  - Henrico County will create individual defense production zones based around individual projects on a case-by-case basis

http://www.vaallies.org/assets/files/incentives/defenseproductionzoneswriteup.pdf

Conclusion

Virginia is proud of its distinguished history and exemplary record of national leadership through exceptional cyber security operations in support of state agencies and operations. The Commonwealth is resolute in its dedication to garnering the expertise of leaders in cyber security in order to mitigate risks. By ensuring the highest level of security for government infrastructure networks, fostering cyber security education and awareness, incorporating innovative best practices to protect data statewide, bolstering business investment with public-private partnerships, and proactively enhancing its national standing as one of the preeminent leaders in the cyber security arena, the Commonwealth leads the nation for cyber security policy.

It's also clear that the Commonwealth of Virginia has developed a world leading technology ecosystem founded on private industry innovation and public-private partnerships. Reflected in the strong presence of state, federal, military, and private cyber security businesses, assets, and activities throughout the Commonwealth, Virginia has leveraged its unique resources and relationships to create this ecosystem of innovation that underpins thriving industry development. Leaders from business, government, and higher education have joined in a shared vision that the Commonwealth will not only to continue to lead the nation in the adoption of signature Information Communication Technologies (ICTs), but to formulate and promote their creation through innovation, investment, and a pro-business environment that nurtures all companies.

The Commonwealth stands as an able and active partner that facilitates the types of innovation that have made the Commonwealth the home of the top technology companies and the number one recipient of federal investment. A shared vision for pro-business policies, a highly skilled workforce, a world-class education system, and cutting-edge technology research have put Virginia squarely at the forefront of cyber security.

Innovation and rapid technology change dominate all markets and all networks, providing ample opportunities for attack, malicious activities, and the degradation of the very systems needed to support society in this interconnected world. The Commonwealth of Virginia understands the devastating impact that neglecting these cyber security challenges poses, and has made it a primary goal to provide an environment for leaders to find partners, companies to find infrastructure and investment, and adversaries to find impenetrable defenses.■

cyberva.virginia.gov