

## University of Washington School of Law UW Law Digital Commons

---

Technology Law and Public Policy Clinic

Centers and Programs


---

6-15-2017

# Employer Liability and Bring Your Own Device: Do Existing Regulations Support Employer Liability for a Compromised Personal Device?

Beth A. Hutchens

Follow this and additional works at: <https://digitalcommons.law.uw.edu/techclinic>

 Part of the [Computer Law Commons](#), and the [Labor and Employment Law Commons](#)

---

### Recommended Citation

Beth A. Hutchens, *Employer Liability and Bring Your Own Device: Do Existing Regulations Support Employer Liability for a Compromised Personal Device?*, (2017).

Available at: <https://digitalcommons.law.uw.edu/techclinic/12>

This Book is brought to you for free and open access by the Centers and Programs at UW Law Digital Commons. It has been accepted for inclusion in Technology Law and Public Policy Clinic by an authorized administrator of UW Law Digital Commons. For more information, please contact [cnyberg@uw.edu](mailto:cnyberg@uw.edu).

**Employer Liability and Bring Your Own Device:  
Do Existing Regulations Support Employer Liability for a Compromised Personal Device?**

By  
Beth A. Hutchens

Candidate for Master of Laws  
in  
Privacy and Public Policy

Law B557

Submitted to Professors William Covington & Dana Raigrodski  
University of Washington School of Law  
Seattle, Washington

**June 2017**

# Contents

Abstract .....	3
I. Introduction .....	4
II. Bring Your Own Device Background.....	5
A. Personal Devices in the Workplace are Favored.....	5
B. There are Significant Risks Associated with BYOD .....	6
C. Many Companies Engage in BYOD Whether They Know it or Not .....	9
III. Finding the Basis for BYOD Liability.....	10
A. Federal Enforcement Actions.....	11
B. State Enforcement Actions .....	12
C. Establishing a Private Plaintiff’s Cause of Action .....	15
1. Proving Redressable Harm that Stems from a Data Breach.....	16
D. BYOD is Beginning to Emerge as a Topic of Concern for States .....	18
IV. Making the Case for Imposing Liability in BYOD - California and Massachusetts.....	19
A. A Potential Jurisdiction for Imposing BYOD Liability: California.....	20
B. Potential Jurisdiction for Imposing BYOD Liability: Massachusetts .....	23
V. Pitfalls and Unintended Consequences of Attaching Employer Liability for Compromised BYOD .....	25
VI: Conclusion .....	26

## **Abstract**

As employers increasingly permit employees to use their personal devices (known as Bring Your Own Device, or “BYOD”) for business purposes, and as the risk of data exposure continues to rise, the question of how, when, and against whom to attach liability remains in flux. This paper will endeavor to explore employer liability as viewed through the lens of hacked or compromised BYOD devices. The research begins by identifying BYOD as a concept along with the risks and benefits incident to the practice. It then discusses current state and federal data protection regulations. It then explores recurring themes in data breach litigation with a particular emphasis on portable device cases. In the remaining parts, the author attempts to discover congruencies in data breach liability and employer liability for portable devices by examining two states with strict data protection regulations that could apply to portable devices regardless of the question of ownership. Lastly, the author identifies the arguments against regulating BYOD devices and suggests that current regulatory frameworks provide ample redress for compromised personal devices used for work purposes.

## I. Introduction

As of January 2017, 95 percent of Americans owned a cellular telephone and 77 percent owned a smart phone.<sup>1</sup> The connectivity of society continues to trend upward while organizations and government agencies continually look for new ways to increase productivity, give employees more flexibility, and cut costs. Permitting employees to use their personal devices for work purposes is one way to accomplish these goals. Commonly referred to as “Bring Your Own Device,” or “BYOD,” it is a term that collectively refers to when employees are allowed to access corporate information and technology resources, such as databases and applications, while using their personal mobile devices like smartphones, laptop computers, and tablet PCs. Put simply, BYOD is a business practice in which employees of an organization are allowed to use their own electronic devices (as opposed to those supplied and/or controlled by the company) to access company information and applications.<sup>2</sup>

BYOD presents unique challenges that are not observed with traditional company-controlled, wired devices such as desktop computers. In the absence of a federal data protection framework, states have begun carve out their own regulatory approaches to data security that affect portable and wireless devices, including those used for BYOD purposes. What has emerged is an inconsistent approach toward addressing portable devices in the workplace, regardless of ownership and control, with no clear indication as to what, if any, issues presented by BYOD can (or should) be addressed by existing regulatory frameworks.

---

<sup>1</sup> Pew Research Center, *Mobile Fact Sheet*, <http://www.pewinternet.org/fact-sheet/mobile/> (last visited June 5, 2017).

<sup>2</sup> R.I. Ogie, *Bring Your Own Device: An Overview of Risk Assessment*, Smart Infrastructure Facility, U. of Wollongong, Wollongong NSW, Australia (2016), citing E. B. Koh, J. Oh, and C. Im, *A Study on Security Threats and Dynamic Access Control Technology for Byod, Smart-Work Environment*, Proc. Int. MultiConf., vol. II, Hong Kong, Mar. 12–14, 2014.

## II. Bring Your Own Device Background

The phrase “Bring Your Own Device” is thought to have first appeared in 2009 when senior management at Intel discovered some employees were using their personal devices at work.<sup>3</sup> Recognizing that the practice dramatically increased productivity, the company embraced it and other organizations soon followed suit—a 2012 study conducted by Cisco showed that 70 percent of workers that handle or use information in the United States use their personal devices at work.<sup>4</sup> The term now refers to more than just cellular telephones—it has evolved to mean any type of device that an employee owns and uses for dual purposes. This often includes tablets, laptops, and wearable devices like Google Glass® and Fit Bit®.<sup>5</sup>

### A. Personal Devices in the Workplace are Favored

BYOD is generally looked upon favorably by senior management and the overarching attitude appears to be that the increased productivity and reduced operating costs that BYOD facilitates, by far, outweigh the added risks. Cisco discovered in 2016 that 66% of IT decision makers polled felt that BYOD is a good thing and that workers save an average of 81 minutes per week when permitted to use their own devices.<sup>6</sup> Cutting corporate costs are also an important part of BYOD because employees bear at least some, if not all, of the costs associated with the

---

<sup>3</sup>*Improving Security and Mobility for Personal Devices*, Intel Best Practices, IT Consumerization, (Feb, 2012),

<http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/improving-security-and-mobility-for-personally-owned-devices-paper.pdf>.

<sup>4</sup> *BYOD: A Global Perspective: Harnessing Employee-Led Innovation*, Cisco Survey Report, (2012), [http://www.cisco.com/c/dam/en\\_us/about/ac79/docs/re/BYOD\\_Horizons-Global.pdf](http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf).

<sup>5</sup> See, generally, Dean Evans, *What is BYOD and Why is it Important? The Opportunities and Risks of People Using Their Own Devices at Work*, (Oct. 7, 2015), Tech Radar,

<http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important-1175088>.

<sup>6</sup> Cisco 2016 Annual Report, <http://www.cisco.com/c/en/us/about/annual-reports.html>.

device.<sup>7</sup> Employees like it too, listing the ability to blend their personal and work lives seamlessly as one of the key benefits of BYOD.<sup>8</sup> They also preferred to use the same device for work as they use in their personal lives and reported being happier and more satisfied with their work when they could choose their own device.<sup>9</sup>

## **B. There are Significant Risks Associated with BYOD**

What is often overlooked or ignored, however, is the fact that there are significant risks associated with BYOD. These risks are numerous, complex, continually changing, and occur in a regulatory environment that is still evolving.<sup>10</sup> In fact, the practice is often jokingly referred to as “bring your own disaster.”<sup>11</sup> The reasons for the increased risks are varied, but BYOD is unique in that personal data is comingled with company data, which adds an extra layer of complexity that goes beyond traditional device protocols. Further, it provides multiple opportunities for data security failures because the devices themselves are often unsecured.

---

<sup>7</sup> This may not always be the case moving forward. An August 2014 decision by a California Court of Appeal determined that if employers require California employees to use their personal devices for work purposes, those employees must receive compensation. *Cochran v. Schwan's Home Service, Inc.*, 2014 Cal. LEXIS 10933 (Cal. Nov. 25, 2014), citing California Labor Code section 2802 (“... to be in compliance with (California Labor Code) Section 2802, the employer must pay some reasonable percentage of the employee’s cell phone bill.”).

<sup>8</sup> *BYOD: A Global Perspective: Harnessing Employee-Led Innovation*, Cisco Survey Report (2012), [http://www.cisco.com/c/dam/en\\_us/about/ac79/docs/re/BYOD\\_Horizons-Global.pdf](http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf).

<sup>9</sup> *Id.*

<sup>10</sup> Operational risks are compounded with BYOD because any risk assessment must not only account for the device owner and his or her data, but the data belonging to customers and/ or the public records associated with it. Further, there are many other issues, both good and bad, when it comes to BYOD- employee productivity remains a hotly contested issue, increased strain on the company’s servers and the IT department in particular, rogue employees and intellectual property theft, litigation holds and eDiscovery, as well as emerging technologies like wearables. Each of these issues has several theories of liability associated with it and while there may be some overlap, a thorough discussion of each is well beyond the scope of this paper, which focuses on liability for compromised devices and the inevitable data breach that ensues.

<sup>11</sup> While this paper discusses risks in a negative context, the increased costs incident to creating and implementing a BYOD program and employing still-developing technologies such as mobile device management can also be thought of as positive risks because they present tremendous opportunities for growth and efficiency.

BYOD is also unique in that issues relating legal liability, regulatory scrutiny, data exposure, increased costs and expenses, and potential brand and reputation damage are still being identified and tested.

### **1. Data Privacy and Security in Mobile Devices Remain Problematic**

The overwhelmingly significant risk associated with BYOD is data leakage and/ or exposure resulting from a lost, stolen, or otherwise compromised device.<sup>12</sup> This is very similar to traditional computing devices, but portable devices, particularly mobile devices, present unique security issues. This is due primarily to the fact that current mobile devices lack strong access protocols commonly found in laptops and other types of hosts.<sup>13</sup> Further, portable devices like laptops are vulnerable to exploits stemming from USB drives, bloatware, imperfect security updates, and many others.<sup>14</sup>

In addition to this, the opportunity for inadvertent exposure of sensitive information by, for example, mistakenly sending sensitive information to personal contacts is extraordinarily high. These problems are compounded by the fact that BYOD involves devices requiring a very high level of IT support, regardless of the make, model, age, or type of the device.<sup>15</sup>

---

<sup>12</sup> *Bring Your Own Device: Security and Risk Considerations for Your Mobile Device Program*, Ernst & Young Insights on Governance, Risk, and Compliance (Sept. 2013)

[\\_Bring\\_your\\_own\\_device:\\_mobile\\_security\\_and\\_risk/\\$FILE/Bring\\_your\\_own\\_device.pdf](#).

<sup>13</sup> These hardware and software components are secure by design and are trusted to perform one or more security-critical functions including: measuring and/or verifying software, protecting cryptographic keys, and performing device authentication. For a general discussion of mobile device security problems see *The Role of the National Institute of Standards and Technology in Mobile Security*, National Institutes of Standards and Technology (Aug. 2015), <http://csrc.nist.gov/documents/nist-mobile-security-report.pdf>

<sup>14</sup> Paul Rubens, *Ten Steps You Can Take to Secure a Laptop*, TechRadar.Pro (May, 2013), <http://www.techradar.com/news/mobile-computing/laptops/10-ways-to-secure-a-laptop-1148348>.

<sup>15</sup> It is worth mentioning that the risks associated with BYOD are compounded in the event of a disgruntled former employee or rogue current employee. In some cases, the control failures and risk mitigation associated with these types of events share some similarities with the actions of



Further, unlike other types of computing devices, BYOD means that personal and company data are permitted to exist on the same device, which creates at least two conflicting interests when it comes to risk management. Among other things, this pits personal autonomy and privacy of the employee at odds with the controls necessary to safeguard company data. Not only is the employee's personal data exposed, but if that employee has access to email, company infrastructure, confidential documents, and other sensitive information, there is an added layer of exposure.<sup>16</sup> As a result, BYOD presents a very real possibility that sensitive data will not only be leaked; it will be hemorrhaged.

Finally, while the cadre of risk factors that accompany these practices fit into traditionally defined categories -people, processes, systems, and external events- there is a uniqueness to BYOD that causes the risks and control failures involved to become increasingly intertwined. For example, a single event- such as ransomware<sup>17</sup> - involves an external force in the form of an

---

“innocent” personnel, but a thorough discussion of how to prevent these types of events is beyond the scope of this paper. For a general discussion of BYOD security and personnel best practices, see Murugiah Souppaya and Karen Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, Nist Special Publication 800-46 Rev. 2 (Jul. 2016), <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>.

<sup>16</sup> It is worth mentioning that the privacy implications with any mobile device are numerous and complex. This paper only contemplates the privacy issues that pertain to data subjects who are not the owner of the device. Thus, while there may be some overlap, the focus of this paper is on members of the public as opposed to employees. Similarly, the liability analysis necessarily changes in the context of intentional acts- such as those by a rogue employee. This paper does not address those issues and instead focuses on purely negligent behavior that results in data exposure. Further, certain types of data are regulated more heavily than others have very clear guidelines and a litany of case law that provides guidance- such as health information and financial information. Given the sheer volume of this topic, the focus of this inquiry has been to explore the potential for liability for exposure of data that is deemed personal, or personally identifiable, but not of the specific types such as medical records or credit card numbers, geolocation, sexual orientation, and other sensitive information.

<sup>17</sup> Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file

individual or group of individuals hijacking a user's computer, a personnel failure at the hands of the person who unwittingly clicked the link, a process failure in the form of a lack of education to help the employee identify suspicious emails, and a system failure in the form of an as yet unknown exploit. Broadly defined, the risk associated with BYOD leads back to leakage and/or exposure of sensitive data belonging to the public, the employee, or in some cases, both.

Accordingly, while it is true that the "risk" associated with BYOD is always the broad concept of data exposure, an analysis that only looks into ways to prevent or mitigate that (and only that) is incomplete and misses the big picture because it focuses too much on an IT solution as opposed to a companywide, systemic approach.

### **C. Many Companies Engage in BYOD Whether They Know it or Not**

BYOD is not a practice that is well defined, or in some cases, understood. Further, employees will use their personal devices at work without permission, training, or rules from managers, stakeholders, or even regulatory authorities. While 80 percent of workers reportedly receive one or more corporate-issued devices, 23 percent of employees surveyed are given corporate-issued smartphones or corporate-issued mobile devices, with more than half of employees who used smartphones at work reporting that they work solely on their personally owned smartphones.<sup>18</sup> What has emerged is a trend for employees to use their personal devices for work purposes regardless of whether there is a company policy, standard operating procedure, and with or without the company's knowledge or permission.

---

types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

<sup>18</sup> *User Survey Analysis: Mobile Device Adoption at the Workplace is Not Yet Mature*, based on 2016 Gartner Personal Technologies Study, Gartner, Inc. (2016), <http://www.gartner.com/newsroom/id/3528217>.

The reality is that BYOD occurs whether management knows it or not, which results in a general attitude of denial or willful ignorance when it comes to personal devices in the public workplace. In 2015, mobile security company Lookout analyzed 20 federal agencies and discovered 14,622 Lookout-enabled devices associated with government networks, despite the lack of permission or a BYOD policy in place for that agency. In another survey of a thousand federal employees, Lookout found that 37 percent said they are willing to sacrifice government security to use a personal device at work despite understanding security concerns, and 40 percent of those working at agencies with policies preventing the use of personal smartphones admitted the rules have little to no impact on their behavior. Lookout's State of Federal BYOD report also found that 24 percent of employees install apps from places other than official app stores, and that 18 percent reported encountering malware on their devices.<sup>19</sup>

It is an accepted truism that, when it comes to cyber incidents, it is not a question of if one will occur, it is a matter of when. With that in mind, while external actors are a driving force that should be accepted as fact and while cyber security is always at the forefront, BYOD has a real potential to be the source of significant employer liability, regardless of how the breach occurred, who owned the device, or what the circumstances were.<sup>20</sup>

### **III. Finding the Basis for BYOD Liability**

Attaching liability for a data breach resulting from a compromised portable device is not unheard of. The unanswered question remains as to what happens when an employee uses her

---

<sup>19</sup> *Feds: You Have a BYOD Program Whether You Like it or Not*, 2015 Lookout State of Federal BYOD Report, [https://media.scmagazine.com/documents/144/fed\\_byod\\_report\\_35977.pdf](https://media.scmagazine.com/documents/144/fed_byod_report_35977.pdf).

<sup>20</sup> It is interesting to note that BYOD is not as prevalent in Europe and Canada. As cross border data transfers become more prevalent, and as the United States struggles to remain compliant with international security and privacy regulations, the question remains as to whether BYOD will decline in popularity for practical reasons. This is especially true when considering the European General Data Protection Regulation that goes into effect in 2018 that requires, among other things, Privacy by Design.

personal device and that device is lost, stolen, or otherwise compromised. If this was done without the company's knowledge or consent, then liability (at least in theory) could be hard to attach under traditional notions of respondeat superior and common law and the laws of agency.<sup>21</sup> If however, as is common, an employee uses her device on behalf of an employer who knows about it, but has no BYOD program, training, or protocol to speak of, does that give rise to a presumption that use of the device was in the scope and in furtherance of the company's interest? Some indicators point to yes, and those indicators don't necessarily turn on traditional notions of common law vicarious liability.<sup>22</sup>

#### **A. Federal Enforcement Actions**

Federal regulatory agencies such as the Federal Trade Commission can and do bring enforcement actions for data breaches under the Privacy Act and various data-specific privacy and security statutes.<sup>23</sup> While not all of such enforcement actions involve lost or stolen portable devices like laptops, tablets, or cell phones, cases involving such devices are not unheard of.<sup>24</sup>

---

<sup>21</sup> For example, sometimes employees install software specifically designed to circumvent company security measures or otherwise use unapproved and insecure services such as cloud storage and open WIFI connections. Employer liability in those cases might not attach, especially if the company had thorough, complete, and established BYOD practices. This will depend greatly on the jurisdiction and will likely turn on state-based theories of tort liability that go beyond the scope of state or federal data security regulations.

<sup>22</sup> This is not to suggest that common law liability is *precluded* with respect to compromised BYOD. Rather, attaching employer liability for data breaches appears to have sufficient basis in device-neutral state and federal data protection regulations that may make such an inquiry unnecessary or, in some cases, imperfect.

<sup>23</sup> *E.g.*, The Children's Online Privacy Protection Act (16 CFR 32), The Gramm Leach Bliley Act, The Health Insurance Portability and Accountability Act, and other data-centered privacy regulations.

<sup>24</sup> *See, for example, in re Accretive Health, Inc* (Federal Trade Commission No. C-4432 (Feb. 5, 2014)(finding the defendant created unnecessary risks of unauthorized access or theft of personal information by transporting laptops containing personal information in a manner that made them vulnerable to theft or other misappropriation), <https://www.ftc.gov/system/files/documents/cases/140224accretivehealthdo.pdf>.

The FTC focuses on the lack of, or otherwise poor, practices and methods which lead to the breach and there is no reason to believe it will decline to bring an enforcement action against a company for data breaches that originate in a portable device, regardless of that device's ownership. This is especially true in light of the fact that the FTC has expressed a keen interest in mobile privacy disclosures, which has a direct bearing on BYOD practices.<sup>25</sup> However, as more and more states begin to pass their own data protection statutes, it stands to reason that a federal enforcement action for compromised BYOD will be in tandem, if at all, with a state action, especially where that state affords greater data protection for consumers.

## **B. State Enforcement Actions**

Forty-eight states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.<sup>26</sup> The provisions vary greatly with respect to who must comply with the law, what falls into the category of "personal information," what constitutes a breach, the specific requirements for notice, and what, if any, exemptions exist.<sup>27</sup> More than half the states have enacted data disposal laws that require entities to destroy or dispose of personal information so that it is unreadable or indecipherable<sup>28</sup>

---

<sup>25</sup>*Mobile Privacy Disclosures: Building Trust Through Transparency*, Federal Trade Commission (Feb. 2013), <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>.

<sup>26</sup>*Security Breach Notification Laws*, National Conference of State Legislatures, <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>, *last visited* June 12, 2017.

<sup>27</sup> *Id.*

<sup>28</sup> Those states are: Alaska (Alaska Stat. § 45.48.500 et seq.); Arizona (Ariz. Rev. Stat. § 44-7601- applies to paper records only); Arkansas (Ark. Code § 4-110-103 Ark. Code § 4-110-104); California (Cal. Civ. Code §§ 1798.81, 1798.81.5, 1798.84- does not apply to government entities); Colorado (Colo. Rev. Stat. § 6-1-713); Connecticut (Conn. Gen. Stat. § 42-471- does not apply to government entities); Delaware (Del. Code tit. 6 § 5001C to -5004C, tit. 19 § 736-

and at least 12 states have laws that apply to private entities.<sup>29</sup> Most of these data security laws generally require businesses that own, license, or maintain personal information about a resident

---

applies to government employers); Florida (Fla. Stat. § 501.171(8)-does not apply to government entities); Georgia (Ga. Code § 10-15-2-does not apply to government entities); Hawaii (Haw. Rev. Stat. §§ 487R-1, 487R-2, 487R-3); Illinois (20 ILCS 450/20, 815 ILCS 530/30, 815 ILCS 530/400); Indiana (Ind. Code §§ 24-4-14-8, 24-4.9-3-3.5(c)-does not apply to government entities); Kansas (Kan. Stat. § 50-7a01, Kan. Stat. § 50-7a03, Kan. Stat. § 50-6, 139b(2); Kentucky (Ky. Rev. Stat. § 365.725-does not apply to government entities); Massachusetts (Mass. Gen. Laws Ch. 93I, § 2); Maryland (Md. State Govt. Code §§ 10-1301 to -13030); Michigan (MCL § 445.72a); Montana (Mont. Code Ann. § 30-14-1703-does not apply to government entities); Nevada (Nev. Rev. Stat. § 603A.200-does not apply to government entities); New Jersey (N.J. Stat. § 56:8-161, N.J. Stat. § 56:8-162); New York (N.Y. Gen. Bus. Law § 399-H-does not apply to government entities); North Carolina (N.C. Gen. Stat. § 75-64-does not apply to government entities); Oregon (Ore. Rev. Stat. § 646A.622); Rhode Island (R.I. Gen. Laws § 6-52-2-does not apply to government entities); South Carolina (S.C. Code § 37-20-190, S.C. Code 30-2-310); Tennessee (Tenn. Code § 39-14-150(g)-does not apply to government entities); Texas (Tex. Bus. & Com. Code § 72.004, § 521.052-does not apply to government entities); Utah (Utah Code § 13-44-201-does not apply to government entities); Vermont (9 Vt. Stat. § 2445-does not apply to government entities); Washington (Wash. Rev. Code § 19.215.020); Wisconsin (Wisc. Stat. § 134.97- Applies to financial institutions, medical businesses or tax preparation businesses); and Puerto Rico (2014 Law #234-2014). NCSL, “Data Disposal Laws”, Dec. 1, 2016 *available at* <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>.

<sup>29</sup> Arkansas (A person or business that acquires, owns or licenses personal information must implement and maintain reasonable security procedures and practices appropriate to the nature of the information); California (A business that owns, licenses, or maintains personal information and third party contractors must implement and maintain reasonable security procedures and practices appropriate to the nature of the information); Connecticut (an individual, business or other entity that is receiving confidential information from a state contracting agency or agent of the state pursuant to a written agreement to provide goods or services to the state must implement and maintain a comprehensive data-security program (as specified/detailed in statute) including encryption of all sensitive personal data transmitted wirelessly or via a public Internet connection, or contained on portable electronic devices has to be encrypted as well, Any person in possession of personal information must safeguard data, computer files and documents); Florida (Covered entities (sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity) and third-party agent (entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity) must take reasonable measures to protect and secure data in electronic form containing personal information); Indiana (a data base owner is a person that owns or licenses computerized data that includes personal information must implement and maintain reasonable procedures, including taking any appropriate corrective action); Kansas (A holder of personal information: a person who, in the ordinary course of business, collects, maintains or possesses, or causes to be collected, maintained or possessed, the personal information of any other person must implement

of that state to implement and maintain reasonable security procedures and practices appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.<sup>30</sup>

---

and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure); Maryland (A business: a sole proprietorship, partnership, corporation, association, or any other business entity (including financial institutions, nonaffiliated third parties / service providers, whether or not organized to operate at a profit must implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations); Massachusetts (Any person that owns or licenses personal information, Authorizes regulations to ensure the security and confidentiality of customer information in a manner fully consistent with industry standards. The regulations shall take into account the person's size, scope and type of business, resources available, amount of stored data, and the need for security and confidentiality of both consumer and employee information must develop, implement, and maintain a comprehensive written information security program appropriate to (a) the size, scope and type of business; (b) the amount of resources available; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information, (as specified/detailed in regulation, including encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly, and encryption of all personal information stored on laptops or other portable devices)); Minnesota (Internet service providers must take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information); Nevada (A data collector that maintains records which contain personal information and a person to whom a data collector discloses personal information must implement and maintain reasonable security measures (as specified /detailed in statute); Oregon (Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data (as specified /detailed in statute); Rhode Island (A business that owns or licenses computerized unencrypted personal information and nonaffiliated third-party contractors must implement and maintain reasonable security procedures and practices appropriate to the nature of the information); Texas (A business or nonprofit athletic or sports association that collects or maintains sensitive personal information. (Does not apply to financial institutions) must make reasonable procedures, including taking any appropriate corrective action); Utah (Any person who conducts business in the state and maintains personal information. Must implement and maintain reasonable procedures). NCSL- Data Security Laws—Private Sector, Jan. 16, 2017. <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx>.

<sup>30</sup>Id.

Some states have shown a willingness to pursue companies for breaches that occurred in connection with a portable device, typically under the particular jurisdiction's data protection statute and consumer protection laws. However, while data breach enforcement actions are common even at the state level, most of these cases do not necessarily involve portable devices but instead are the result of Internet activities, network vulnerabilities, and the like.<sup>31</sup> Still, even though they are not as common as those involving other types of data breach incidents, there are some instances of state attorneys general bringing actions against companies for data breaches in connection with portable devices, sometimes as the result of employee activity.<sup>32</sup>

### **C. Establishing a Private Plaintiff's Cause of Action**

While a private plaintiff is not entirely without recourse in the event her information becomes compromised, the road to establishing company liability for such a plaintiff (or group of plaintiffs) has not been an easy one to traverse. As a threshold matter, only a handful of states permit a private cause of action, while the vast majority leave data breach lawsuits solely

---

<sup>31</sup> There are many such cases, however the largest to date involves the 2013 Target Corporation data breach, where the company recently settled with 47 states and the District of Columbia to the tune of \$1.8 million for a breach that occurred when a network vulnerability exposed financial and/ or personal information of 100 million customers.

<sup>32</sup> *See, for example in re Kaiser Foundation*, Stipulation for entry of final judgment and permanent injunction, No. No. RG14711370 (Cal. Super. Feb. 14, 2014) (consenting to judgment after an unencrypted USB drive was discovered at a thrift store that contained over 20,000 employee records), [https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/kaiser\\_stipulation.pdf](https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/kaiser_stipulation.pdf); *Commonwealth v. Beth Isr. Deaconess Med. Ctr.*, 2014 Mass. Super. LEXIS 2250 (Mass. Super. Ct. Nov. 20, 2014) (allegations that the defendant violated state and federal law, including by not properly protecting PHI and PI stored on an unencrypted laptop, not physically securing that laptop, not properly training its employees, and not providing timely notification of the incident when the laptop was stolen and requiring administrative procedures requiring each workforce member who uses, stores, or maintains PHI or PI on a personally owned laptop computer to encrypt such device).



within the discretion of the state attorney general.<sup>33</sup> Further, individuals seeking to recover damages when their information has been exposed must have standing and must be able to demonstrate concrete harm. Historically, this has been difficult to establish without a showing of actual misuse of that person's data, but in recent months, courts have been more willing to entertain, and even loosen, the standards of showing harm resulting from compromised data.

### **1. Proving Redressable Harm that Stems from a Data Breach**

Private data breach plaintiffs must be able to demonstrate that they have suffered, or will suffer some harm at the hands of the defendant that is redressable by the court.<sup>34</sup> Historically, private plaintiffs in data breach cases have struggled to show that the loss or exposure of their personal information is an actual, non-hypothetical injury. And courts continue to wrestle with the issue since the United States Supreme Court's discussion of the concreteness requirement in *Spokeo, Inc. v. Robbins*<sup>35</sup> and have reached inconsistent outcomes according to different interpretations and individual state standards for private data breach plaintiffs. As a result, there is a split of authority over when and how private data breach plaintiffs can bring suit.

For the most part, the standing question is easiest to answer when a plaintiff can show actual misuse of his data following a breach. This typically requires showing that the plaintiff's

---

<sup>33</sup> The states that permit private data breach suits are: Alaska, California, Louisiana, Maryland, Massachusetts, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Texas, Virginia, Washington, the District of Columbia, Puerto Rico, and the Virgin Islands.

<sup>34</sup> The concept of standing enjoys a rich jurisprudential history at both the state and federal levels. Put simply, Standing, or locus standi, is capacity of a party to bring suit in court. State laws define standing. At the heart of these statutes is the requirement that plaintiffs have sustained or will sustain direct injury or harm and that this harm is redressable. *Standing*, WEX LEGAL DICTIONARY, Legal Information Institute, Cornell Law School, <https://www.law.cornell.edu/wex/standing>, last visited July 12, 2017.

<sup>35</sup> 136 S. Ct. 1540, 194 L. Ed. 2d 635 (2016).

personal information was used in some fashion that caused actual, or impending harm.<sup>36</sup>

However, in cases where there has been a breach and data has been merely exposed, as opposed to used in some fashion, or in cases where the plaintiff struggles with showing that such a use is imminent, a split of authority has emerged. Most courts hold that a plaintiff who cannot demonstrate actual or imminent injury cannot show concrete harm sufficient to confer standing because the fact that the data might be used at some unidentifiable point in the future is not sufficient to show imminent injury.<sup>37</sup> However, some courts are willing to entertain a more

---

<sup>36</sup> See, for example, *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.D.C. 2014) (finding that two plaintiffs had asserted the requisite injury-in-fact when one began receiving unsolicited telephone calls pitching medical products and services targeted at her specific medical condition the second received mail indicating that he had applied for a loan that he did not apply for, and that his credit history had been adversely affected as a result); *Corona v. Sony Pictures Entertainment, Inc.*, No. 14-CV-09600 RGK, 2015 U.S. Dist. LEXIS 85865 (C.D. Cal. June 15, 2015) (finding that allegations that plaintiffs' information had been stolen, posted on file sharing sites, and used to send threatening e-mails to former Sony employees and their families were sufficient to confer standing); *In re Adobe Systems Privacy Litigation*, 66 F.Supp. 3d 1197, 1213 (N.D. Cal. 2014). (Finding that *Clapper v. Amnesty Intern., USA*, U.S., 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013) did not overrule any precedent or reformulate the familiar standing requirements, that the plaintiffs' allegations were sufficiently concrete and imminent to show a substantial risk of future harm, that their allegations relating to the cost of mitigating this risk constituted an additional cognizable injury, and that that there was no need to speculate as to whether their information had been stolen by someone who intended to misuse, and was capable of misusing, their data in light of the fact that some of the stolen information had already surfaced on the Internet, and that the hackers had used the defendants own systems to decrypt credit card numbers.); *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 665 (E.D. Pa. 2015) (holding the plaintiff had standing where his credit cards and bank accounts had actually been misused by thieves because harms are not "future harms," but ongoing, present, distinct, and palpable).

<sup>37</sup> See, For example, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40 (3d Cir. 2011)(declining to confer standing based on the argument that a breach increased the risk of identity theft and holding that the plaintiffs alleged injury was not imminent and was instead based on a hypothetical risk of harm that depended on the actions of an unknown third party); *Kamal v. J. Crew Grp., Inc.*, 2016 U.S. Dist. LEXIS 145392 (D.N.J., October 20, 2016) (refusing to find standing because there was no evidence that anyone has accessed or attempted to access or will access Plaintiff's credit card information); *In re Cmty. Health Sys.*, 2016 U.S. Dist. LEXIS 123030, N.D. Ala. Sept. 12, 2016) (recognizing a split in the circuits with respect to Article III standing and finding that actual harm may occur only if the hacker is able to decrypt and convert the information hacked to some understandable and usable form; if the hacker intends to commit future criminal acts by

permissive approach toward conferring standing, finding that the risk of imminent harm posed by the data breach itself is sufficient.<sup>38</sup>

The result is that where defendants in data breach actions could once readily dismiss data breach cases by challenging the plaintiff's standing, they are now finding that courts in some jurisdictions do not so readily accept such an argument. This leads to a higher likelihood that data breach cases are being examined more closely and inquiries into the defendant's cybersecurity practices will increase. As the trajectory for mobile and portable device usage for work purposes continues to trend upwards, it stands to reason that more and more jurisdictions will begin to address the company's practices- not necessarily from a device-specific standpoint as in the case with BYOD, but from a company policy standpoint, with the standard of demonstrating harm becoming easier to meet. Thus, a company engaging in BYOD may find not only its data security practices called into question, but also whether, and to what extent, those practices can be attributable to the plaintiff's injury.<sup>39</sup>

#### **D. BYOD is Beginning to Emerge as a Topic of Concern for States**

The above discussion should not be taken to suggest that BYOD is of no great concern for state or local governments and it certainly doesn't mean that there is not a colorable argument for establishing employer liability for personally owned devices. Many states have been pushing for comprehensive BYOD programs for quite some time and others have implemented

---

misusing the information or selling it to another who so intends; and if the hacker or those who may obtain the personal information are indeed able to successfully make unauthorized use of it) citing *Clapper v. Amnesty Intern., USA, U.S.*, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013).

<sup>38</sup> See e.g., *Remijas v. Neiman Marcus Group*, 794 F.3d 688, 689 (7th Cir. 2015). (holding that the plaintiffs presented a non-speculative risk of harm that created standing when they spent time and money resolving fraudulent charges and protecting against future identity theft. In determining that the breach presented an imminent risk of harm, the Seventh Circuit questioned why else would hackers steal a consumer's PII or identity if not to make fraudulent charges).

<sup>39</sup> *Coca Cola*, *supra* note 36. The facts in *Coca Cola* involved a stolen laptop that contained employees' PII.

at least some level of guidance.<sup>40</sup> Further, there have been at least a few attempts by state legislatures to enact some sort of regulation that addresses BYOD in some limited circumstances.<sup>41</sup> While these programs almost exclusively address BYOD in government agencies, and proposed legislation has not seen any remarkable success, it is safe to assume that the issues BYOD presents are no longer unacknowledged or ignored.<sup>42</sup>

#### **IV. Making the Case for Imposing Liability in BYOD - California and Massachusetts.**

Though the states' approach to data security and BYOD remain varied, liability for data breaches share some commonality in that lawsuits (both public and private) for the harms suffered as the result of a breach are on the rise. And it appears that these cases turn on the breach itself, as opposed to whether it came from a portable device or not. However, courts do not appear terribly concerned with who caused the breach and more with how it was breached, they may focus on the breach itself, as opposed who owned the device. As more and more states adopt forward thinking strategies with respect to technology, this trend will likely continue

---

<sup>40</sup> See, for example, State of Rhode Island Department of Administration, *Mobile Device Security* (2016), <http://www.doit.ri.gov/documents/policies/MobileDeviceSecurity.pdf>; State of Oklahoma Office of Management and Enterprise, *Bring Your Own Device Agreement*, <https://www.ok.gov/cio/documents/BringYourOwnDeviceAgreement.pdf>, last visited June 6, 2017; State of Indiana *Policy and Procedures for Use of Personally Owned Mobile Devices to Access the Information Resources of Indiana State Government: A Semimanaged BYOD Program*, [https://www.in.gov/iot/files/Mobile\\_Device\\_Policy\\_with\\_BYOD.pdf](https://www.in.gov/iot/files/Mobile_Device_Policy_with_BYOD.pdf) last visited June, 8, 2017.

<sup>41</sup> See, e.g., State of North Carolina Session Law 2013-360, Senate Bill 402 sec. 7.18 (d)(directing the Office of the Chief Information Officer to develop a policy for implementing a "bring your own device" (BYOD) plan for state employees),

<sup>42</sup> There is also substantial guidance regarding BYOD from both the federal government and private industry. See, for example, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*, Murugiah P. Souppaya and Karen Scarfone, NIST SP 800-114 Rev 1 (Jul. 2016), <https://www.nist.gov/publications/users-guide-telework-and-bring-your-own-device-byod-security>; *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged*, U.S. Govt Accountability Off. Rep. to Cong. Comm. (Sept. 2012), <http://www.gao.gov/assets/650/648519.pdf>; David A. Willis, *Bring Your Own Device Program Best Practices (BYOD)*, Gartner Webinar, <https://www.gartner.com/webinar/2392315>.

upward. And, as discussed above, an individual plaintiff or class of plaintiffs will need a statutory basis to bring a suit (as opposed to that state's attorney general). While BYOD presents its own challenges, is more nuanced than traditional devices, and is not always specifically identified, traditional notions of data breach liability do come into play, whether or not there is a colorable argument for liability under the common law. Thus, a cause of action for compromised data as a result from compromised BYOD will likely find its source in jurisdictions that have a strong data protection framework and a willingness to adopt a data-specific (as opposed to device-specific) approach.

#### **A. A Potential Jurisdiction for Imposing BYOD Liability: California**

California has historically enjoyed the spotlight when it comes to forward-looking data protection regulations. One of the first states to adopt a comprehensive regulatory scheme, it has routinely and consistently been a state that others look to for guidance when it comes to regulating emerging technologies and their uses, including personal devices. Its data protection statutes impose a general statutory duty to safeguard personal information<sup>43</sup> and require adherence to strict notification requirements.<sup>44</sup> Further, in California, state agencies must comply with information security programs developed by the Chief of the Office of Information Security, including conducting an annual independent security assessment and implementing cybersecurity strategy incident response standards to secure its critical infrastructure controls and critical infrastructure information.<sup>45</sup> In addition to government agencies, private businesses are also statutorily obligated to safeguard personal information. That is to say, in California, any

---

<sup>43</sup> See *supra* Notes 26 – 28.

<sup>44</sup> California also requires a specific format for breach notification, has an online fillable form for notification, and provides sample notices for guidance. Available at <https://oag.ca.gov/ecrime/databreach/report-a-breach>.

<sup>45</sup> Calif. Govt. Code § 11549.3 et seq., Calif. Govt. Code § 8592.30-8592.45.

business that owns, licenses, or maintains personal information must implement and maintain reasonable security procedures and practices appropriate to the nature of the information.<sup>46</sup> This includes a requirement that businesses who disclose personal information about a California resident to a nonaffiliated third party must 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 unauthorized access, destruction, use, modification, or disclosure.<sup>47</sup>

California is also one of several states that has closed the loophole for breaches of encrypted information, requiring notification when “encrypted personal information is acquired”. This could play a key role in breach liability for portable devices, including BYOD, even though there is not a dearth of jurisprudence in California addressing violations of its data protection statutes that specifically deals with BYOD or even portable devices. However, California courts do appear to have a more permissive attitude with respect to individuals claiming harm from a data breach, as opposed to outright dismissal for lack of standing.<sup>48</sup> And there are some

---

<sup>46</sup> See *Supra* Note 28; Cal. Civ. Code §§ 1798.80 et seq,

<sup>47</sup> *Id.*

<sup>48</sup> See, e.g., *Patton v. Experian Data Corp.*, SACV 15-1871 JVS (PLAX), 2016 U.S. Dist. LEXIS 60590 (C.D. Cal. May 6, 2016) (remanding a class action data breach matter to superior court because the plaintiff’s lacked Art. III standing thus paving the way for the case to be evaluated on the merits); *Walters v. Kimpton Hotel & Rest. Grp., LLC*, 2017 U.S. Dist. LEXIS 57014 Case No. 16-cv-05387-VC (N.D. Cal. Apr. 13, 2017)(disagreeing that a plaintiff must actually suffer the misuse of his data or an unauthorized charge before he has an injury for standing purposes, citing *Lewert*, 819 F.3d at 967-68 (concluding that time and effort spent monitoring card statements and financial accounts were sufficient to confer standing even though the plaintiff had not yet experienced unauthorized charges); see also *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) ( holding that “[T]o require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact.”); but see *Ross v. Cal. Health Care Servs.*, 2017 U.S. Dist. LEXIS 57770 (E.D. Cal. Apr. 14, 2017)(finding that the plaintiff couldn’t show if any information was on a compromised laptop, and if there was, the type, scope, and existence of *his*

cases where courts were willing to impose liability for violation of §1798 in connection with breaches of portable devices.<sup>49</sup>

Despite a relatively small number of data breach cases involving portable devices, BYOD is certainly on California's radar, and in some instances, the practice is not looked upon favorably, at least for government agencies<sup>50</sup>. Further, the California Secretary of State and the Attorney General's Office has acknowledged that personal devices in the workplace raise unique security challenges and has provided guidance to businesses that use BYOD to reduce the threat of data breaches, malware, and other cyber security incidents.<sup>51</sup> Thus, courts in California appear less concerned with the mechanism of a breach (hacking versus phishing versus lost or stolen devices) and are more concerned with whether a company's practices with respect to the data are reasonable. Based on this presumption, it stands to reason that there is at least the possibility that California courts would impose employer liability for a compromised BYOD if

---

information on the laptop and holding that a plaintiff cannot state a claim for relief based upon the speculative breach of his sensitive information).

<sup>49</sup> See for example, *Johansson-Dohrmann v. CBR Sys.*, *Johansson-Dohrmann v. CBR Sys.*, 2013 U.S. Dist. LEXIS 103863, 2013 WL 3864341 (S.D. Cal. July 24, 2013) (approving a class action settlement of a matter involving a breach of confidential health and financial after computer equipment and computer backup tapes containing it were stolen); *Falkenberg v. Alere Home Monitoring, Inc.*, 2015 U.S. Dist. LEXIS 22121, 2015 WL 800378 (N.D. Cal. Feb. 23, 2015) (denying the defendants' motion to dismiss claims relating to a stolen laptop containing their medical information).

<sup>50</sup> "An agency with a BYOD policy is potentially opening a Pandora's Box of legal and privacy issues. If a portable device or laptop computer is needed for an employee to complete essential job duties, best practice would be to issue a state owned device that has the proper IT support to accommodate security and discovery issues", *Electronic Records Guidebook: Personal Devices*, California Secretary of State Archives, <http://www.sos.ca.gov/archives/programs/electronic-records/electronic-records-guidebook/personal-devices/>, last visited 8 June 2017; see also California Department of Justice, Office of the Attorney General Data Breach Report, (Feb. 2016), <https://oag.ca.gov/breachreport2016#notes>.

<sup>51</sup> California Department of Justice, California Office of the Attorney General, *Cybersecurity in the Golden State: How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents* available at <https://oag.ca.gov/cybersecurity>.

the employer's data security standards fell below the minimum requirements imposed by California law.

## **B. Potential Jurisdiction for Imposing BYOD Liability: Massachusetts**

Massachusetts is another state that has robust data security and privacy regulations. In addition to imposing a duty on “any person that owns or licenses personal information about a resident of the commonwealth” to safeguard the personal information of residents of the commonwealth that is consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated.<sup>52</sup> Massachusetts data privacy regulations also have strict notification requirements in the event of a breach that are triggered when the employer knows or has reason to know that a breach has occurred or that an unauthorized person has acquired or used the data for an unauthorized purpose.<sup>53</sup> Further, similar to California, notice must be provided to the state attorney general and the director of consumer affairs and business regulation.<sup>54</sup>

Massachusetts General Law Chapter 93H was implemented by 201 CMR 17.00 and required compliance by 2010.<sup>55</sup> It requires, among other things, those in possession of personal information to have a written information security plan, record identification, risk assessment, third party vetting, and a breach response plan.<sup>56</sup> And, like California, Massachusetts provides significant guidance for companies doing business in Massachusetts to comply with CMR 17.<sup>57</sup>

---

<sup>52</sup> Massachusetts General Laws, Ch. 93H §2.

<sup>53</sup> *Id.* at §3.

<sup>54</sup> *Id.*

<sup>55</sup> §5(1).

<sup>56</sup> Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, *201 CMR 17.00 Checklist*, <http://www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf>, last visited July 12, 2017.

<sup>57</sup> *See id.* *See also* Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, *Frequently Asked Questions Regarding 201 CMR 17.00*,



However, unlike California, the Massachusetts data protection statute only applies to data that is not encrypted, that is, there is a “encryption safe harbor exemption.” Thus, no notice is required as long as the data acquired or used is encrypted, and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information has not been acquired.

However, Massachusetts courts have been willing to impose liability in connection with portable devices. As is common with data breach enforcement actions, these cases overwhelmingly settle, but what has emerged is a pattern, at least in Massachusetts, that suggests Compromised portable devices can be the basis for liability.<sup>58</sup> Massachusetts laws specifically address portable devices, requiring encryption of personal information stored on them<sup>59</sup> and also applies to wireless transmissions.<sup>60</sup> And while actual adjudications are not numerous, there is at

---

<http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf>; (2012), 2010-02; Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation *Compliance with 201 CMR 17:00: Standards for the Protection of Personal Information of Residents of the Commonwealth*, <http://www.mass.gov/ocabr/insurance/providers-and-producers/doi-regulatory-info/doi-regulatory-bulletins/2010-doi-bulletins/2010-02-compliance-with-201-cmr-1700.html>; Office of the Attorney General of Massachusetts, *Guidance for Businesses on Security Breaches* (2017), <http://www.mass.gov/ago/doing-business-in-massachusetts/privacy-and-data-security/security-breaches.html>. The private sector has also weighed in on the matter. *See, for example, Cisco Outlook 201 CMR 17.00 Compliance Guide* (Feb. 2017), <https://resources.cloudlock.com/compliance-guides/mass-201-cmr-17-00-compliance>.

<sup>58</sup> *See, for example, Commonwealth v. Beth Isr. Deaconess Med. Ctr.*, (entering a consent decree in connection with the theft of an unencrypted laptop used by a BEDMC physician, containing the PHI of nearly 4,000 Massachusetts residents and PI of approximately 230 employees of BEDMC or its affiliate); *Commonwealth v. Women & Infants Hosp. of R.I.*, 2015 Mass. Super. LEXIS 1234 (Mass. Super. Ct. Sept. 24, 2015)(Consent decree in connection with an action alleging the defendant engaged in unfair or deceptive acts or practices, including not properly protecting PI and PHI, that was stored on unencrypted back-up computer tapes that were shipped off-site).

<sup>59</sup> Mass. Regs. Code tit. 201, §§ 17.03 – 17.04

<sup>60</sup> §§ 17.04.

least some small hint that Massachusetts will pursue companies whose device practices fail to meet Massachusetts cybersecurity and encryption requirements.<sup>61</sup>

If anything can be learned from states like Massachusetts and California it is that there appears to be a growing trend for courts imposing liability, not based on the type of device, or who owned it, but for violation of the data breach statutes in general. Thus, attaching liability for a portable device in Massachusetts, California, (or other states with similar approaches to data protection) will likely not turn on ownership of the device itself, or even the type of device, but rather how and when a breach occurred.

#### **V. Pitfalls and Unintended Consequences of Attaching Employer Liability for Compromised BYOD**

With respect to BYOD and liability for compromised personal devices, there is much left to discover with respect to use cases, federal, state, and local regulations, device and application security, privacy and security, and a cadre of other issues. Thus, arguably, any attempt to draft a comprehensive set of regulations is an exercise in futility. Further, the speed with which regulations slog through the legislative process coupled with the rapidly evolving technology and uses of personal devices all but guarantees near-instant obsolescence for any regulation that manages to see the light of day.

Further, however admirable the intentions might be, the reality is that not every company can afford to implement increasingly strict measures, especially those who only have a handful of devices. Arguably, comprehensive regulatory schemes could inadvertently shut the door for businesses that want to use BYOD but don't have the resources to adhere to the many

---

<sup>61</sup> Attorney General of Massachusetts Press Release, *Property Management Firm to Pay \$15,000 in Civil Penalties Following Data Breach: Laptop Containing Personal Information of Over 600 Residents Stolen* (2012), <http://www.mass.gov/ago/news-and-updates/press-releases/2013/140k-settlement-over-medical-info-disposed-of-atdump>.

requirements. And, since states are adopting their own unique approaches, this forces companies doing interstate business to adhere to different, and sometimes, conflicting requirements which may inspire them to scrap the practice altogether. This is not the most pragmatic way of approaching the problem, and if a company takes a data-centered approach, there is at least a colorable argument that protocols and practices are already covered by the (ever growing) list of regulations that focus not so much on a device, but the data it contains, thus, any rule specific to BYOD could be superfluous, redundant, and/ or unnecessary.

The current political climate has encouraged state attorneys general to create their own approaches toward data privacy and security. And it is entirely possible that BYOD may be folded in to existing data practices, thus any attempt to codify device-specific rules is superfluous, overly burdensome, and completely unnecessary. Thus, it might be best, at least for the time being, to employ existing regulations according to data type, as that would allow for improvements to technology without hamstringing innovation and commerce. Any attempts to regulate a rapidly changing and still developing area such as BYOD would be premature, imperfect, and in all probability, ineffective. Further, a draconian enforcement protocol at either the state or federal level would likely result in companies being skittish about permitting BYOD at all. This may not be the most realistic approach to BYOD if the goal is to combine technology and business in meaningful and positive ways.

## **VI: Conclusion**

Permitting employees to use their personal devices for work purposes presents unique challenges that are not present in traditional company-controlled, wired devices such as desktop computers. In the absence of a federal data protection framework, states have begun to carve out their own regulatory approaches, including those that include or affect portable and wireless

devices like BYOD. What has emerged is an inconsistent approach toward addressing portable devices, regardless of ownership and control, with no clear indication as to what, if any, issues presented by BYOD can or should be addressed by existing regulatory frameworks.

BYOD is generally looked upon favorably by senior management and employees alike. What is often overlooked or ignored, however, is the fact that there are significant risks associated with BYOD that are numerous, complex, continually changing, and occur in a continuously evolving regulatory environment. And BYOD is unique in that, unlike company-supplied devices, personal data is comingled with company data, which adds an extra layer of complexity that goes beyond traditional device protocols. The overwhelmingly significant risk associated with BYOD is data leakage and/or exposure resulting from a lost, stolen, or otherwise compromised device. Further, many times, employees use their personal devices at work without permission, training, or rules from managers, stakeholders, or even regulatory authorities. What has emerged is a trend for employees to use their personal devices for work purposes regardless of whether there is a company policy, standard operating procedure, and to do so with or without the company's knowledge or permission.

Attaching liability for a data breach resulting from a compromised portable device is not unheard of. The unanswered question remains as to what happens when an employee uses her personal device and that device is lost, stolen, or otherwise compromised. If this was done without the company's knowledge or consent, then liability (at least in theory) could be hard to attach under traditional notions of respondeat superior and agency. If, however, as is common, an employee uses her device on behalf of an employer who knows about it, but has no BYOD program, training, or protocol to speak of, it may give rise to a presumption that use of the device

was in the scope and in furtherance of the company's interest, the analysis of which does not necessarily turn on traditional notions of common law vicarious liability.

Federal regulatory agencies such as the Federal Trade Commission can and do bring enforcement actions for data breaches under the Privacy Act and various data-specific privacy and security statutes. While not all of such enforcement actions involve lost or stolen devices like laptops, tablets, or cell phones, cases involving such devices are not unheard of. However, as more and more states begin to pass their own data protection statutes, it stands to reason that a federal enforcement action for compromised BYOD will be in tandem with a state action, especially where that state affords greater data protection for consumers.

Forty-eight states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information, more than half the states have enacted data disposal laws that require entities to destroy or dispose of personal information so that it is unreadable or indecipherable, and at least 12 states have laws that apply to private entities. Most of these data security laws generally require businesses that own, license, or maintain personal information about a resident of that state to implement and maintain reasonable security procedures and practices appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

Some states have shown a willingness to pursue companies for breaches that occurred in connection with a portable device, typically under the particular jurisdiction's data protection statute and consumer protection laws. Even though they are not as common as those involving other types of data breach incidents, there are some instances of state attorneys general bringing

actions against companies for data breaches in connection with portable devices, which sometimes are the result of employee activity.

Private plaintiffs have struggled to maintain viable claims when their information is compromised, but that may be changing. Most courts hold that a plaintiff who cannot demonstrate actual or imminent injury cannot show concrete harm sufficient to confer standing. However, other courts are willing to entertain a more permissive approach toward conferring standing, finding that the risk of imminent harm posed by the data breach itself is sufficient. As the trajectory for mobile and portable device usage for work purposes continues to trend upwards, it stands to reason that more and more jurisdictions will begin to address the company's practices not necessarily from a device-specific standpoint, but from a company policy standpoint, with the standard of demonstrating harm becoming easier to meet.

Though the states' approach to data security and BYOD remain varied, liability for data breaches share some commonality in that lawsuits (both public and private) for the harms suffered as the result of a breach are on the rise. And it appears that these cases turn on the breach itself, as opposed to whether it came from a portable device or not. However, courts do not appear terribly concerned with who caused the breach and more with how it was breached, they may focus on the breach itself, as opposed who owned the device. As more and more states adopt forward thinking strategies with respect to technology, this trend will likely continue upward. This is especially true in jurisdictions that have adopted stricter data protection regulations like California and Massachusetts.

However, with respect to BYOD and liability for compromised personal devices, there is much left to discover with respect to use cases, federal, state, and local regulations, device and application security, privacy and security, and a cadre of other issues. Thus, arguably, any

attempt to draft a comprehensive set of regulations is an exercise in futility. Further, however admirable the intentions might be, the reality is that not every company can afford to implement increasingly strict measures, especially those who only have a handful of devices. Arguably, comprehensive regulatory schemes could inadvertently shut the door for businesses that want to use BYOD but don't have the resources to adhere to the many requirements. And, since states are adopting their own unique approaches, it is entirely possible that BYOD may be folded in to existing data practices, thus any attempt to codify device-specific rules is a wasted effort.

Using one's personal devices for work purposes remains a popular practice with no indication of declining any time soon. In conclusion, BYOD remains a viable business practice, and so long as companies engaging in it adhere to current regulatory frameworks, there is no reason it should be approached any differently than traditional protocols with respect to data security and privacy.