Richmond Journal of Law and Technology

Volume 21 | Issue 3 Article 6

2015

Wherever You Go, There You Are (With Your Mobile Device): Privacy Risks and Legal Complexities Associated with International 'Bring Your Own Device' Programs

Melinda L. McLellan

James A. Sherer

Emily R. Fedeles

WHEREVER YOU GO, THERE YOU ARE (WITH YOUR MOBILE DEVICE): PRIVACY RISKS AND LEGAL COMPLEXITIES ASSOCIATED WITH INTERNATIONAL "BRING YOUR OWN DEVICE" PROGRAMS

By: Melinda L. McLellan,* James A. Sherer,** & Emily R. Fedeles***

Cite as: Melinda L. McLellan, James A. Sherer, & Emily R. Fedeles, *Wherever You Go, There You Are (With Your Mobile Device): An Examination of Privacy Risks and Legal Complexities Associated with Cross-Border "Bring Your Own Device" Programs*, 21 RICH. J.L. & TECH. 11 (2015), http://jolt.richmond.edu/v21i3/article11.pdf.

I. INTRODUCTION

[1] The cross-use of mobile devices for personal and professional purposes—commonly referred to as "Bring Your Own Device" or "BYOD" for short[1]—has created a new backdrop for doing business that was scarcely imaginable even ten years ago. The advertisements for broadening the scope of employee mobile device usage almost write themselves: BYOD is said to give employees the freedom to "work and collaborate the way they prefer" making for a "more mobile, productive,

The views expressed herein are solely those of the authors, should not be attributed to their places of employment, colleagues, or clients, and do not constitute solicitation or the provision of legal advice.

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

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

*** Emily R. Fedeles is an Associate in Shook, Hardy & Bacon's Geneva, Switzerland office.

[1] *See* Eddie D. Woodworth, *The Importance of BYOD Policies: Turning "Bring Your Own [Legal] Disaster" into "Bring Your Own Competitive Advantage"* 3–4 (Dec. 2012) (unpublished manuscript) (on file with author).

and satisfied" workforce.[2] Although BYOD programs do indeed have the potential to reduce expenses and increase productivity for many organizations, the "freedom" associated with BYOD is, in fact, not free: regardless of which party pays for the devices or their service charges, BYOD practices increase compliance challenges for organizations of all sizes.[3] The implementation of a BYOD program generally results in a significant increase in technological and administrative complexity, even for organizations that only do business in one country.[4] For multinationals with employees who regularly travel internationally and have a constant need for seamless, worldwide access to data, the ever-evolving struggle with myriad legal and practical BYOD-related issues is very real.[5]

[2] Listed in 2014 as the "number one e-Discovery challenge . . . for the coming years,"[6] and often presented as a clash between "personal data privacy concerns for the employee" and "cyber security issues on the

[2] *Bring-Your-Own Device: Enable Choice and Simplify IT with BYOD*, CITRIX, http://www.citrix.com/solutions/bring-your-own-device/overview.html, *archived at* http://perma.cc/DMS5-9TLV (last visited Feb. 27, 2015).

[3] *See, e.g.*, Laureen Hicks, *BYOD Management Services: A Critical Need for Enterprises in 2015*, VERIZON ENTER. SOLUTIONS (Nov. 10, 2014), http://news.verizonenterprise.com/2014/11/byod-forrester-wave-mobility-management/, *archived at* http://perma.cc/5Y8G-SZKB.

[4] *See, e.g.*, *id.* (citing CHRIS ANDREWS ET. AL., THE FORRESTER WAVE™: GLOBAL BYOD MANAGEMENT SERVICES, Q2 2014 at 2, (Forrester 2014), *available at* http://www.slideshare.net/VerizonEnterpriseSolutions/forrester-byodreport, *archived at* http://perma.cc/8XNQ-LYPS).

[5] NICHOLAS MCQUIRE, GLOBAL BYOD ATTITUDES AND BEST PRACTICE FOR MULTINATION ORGANISATIONS (IDC 2012), *available at* http://www.vibrantmedia.co.za/m/creativecounsel/vodacomboyd/November2012/IDCWP28U_Web.pdf, *archived at* http://perma.cc/TG48-4RYS.

[6] Erik Hammerquist, *BYOD Is the No. 1 E-Discovery Challenge for 2014*, L.TECH. NEWS (Jan. 16, 2014), *available at* http://autonomy.corporatecounsel.law.com/vendor-voice-byod-is-the-no-1-e-discovery-challenge-for-2014/, *archived at* http://perma.cc/K4A5-HAPM.

corporate side,"[7] BYOD nonetheless appears to be a risk worth the reward for many organizations. Buttressed by encouraging data and compelling marketing, BYOD is touted as "combining workforce mobility and 'always reachable' boosts in employee productivity with possible savings on corporate telecom services and device spending,"[8] while at the same time increasing worker efficiency and satisfaction.[9] BYOD is frequently promoted as a boon to "employees [who] want to use their own smartphones and tablets at work for convenience as the border between work and personal or recreational activities continues to blur."[10]

[3] As virtually everyone who plays a part in the information economy knows from personal experience, mobile devices have become electronic tethers for many of their owners.[11] The data on any given device may originate with the user, an employer, or another third party, or be collected through automatic means (for example, through data logging, geolocation tracking, or built-in motion detectors).[12] The Supreme Court's opinion in *Riley v. California* highlighted the "element of pervasiveness that

[7] *Collision Course Ahead? Personal Data Privacy v. Corporate Security in a BYOD World*, A.B.A. NEWS CRIM. J. SEC. (Aug. 11, 2014), *available at* http://www.americanbar.org/news/abanews/aba-news-archives/2014/08/collision_courseahe.html, *archived at* http://perma.cc/YZZ3-KR3H.

[8] CLAUS HETTING, MITIGATING SECURITY & COMPLIANCE RISKS WITH EMM 4(Heavy Reading 2014), *available at* http://us.blackberry.com/content/dam/bbfoundation/pdf/case-study/na/en/Mitigating_Security_and_Compliance_Risks_with_EMM_Whitepaper_May_2014.pdf, *archived at* http://perma.cc/ZE5Y-BUNU.

[9] *See* Anisha Mehta, Comment, *"Bring Your Own Glass:" The Privacy Implications of Google Glass in the Workplace*, 30 J. MARSHALL J. INFO. TECH & PRIVACY L. 607, 608 (2014), *available at* http://repository.jmls.edu/jitpl/vol30/iss3/6/, *archived at* http://perma.cc/34UF-LZRL.

[10] HETTING, *supra* note 8.

[11] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.").

[12] *See, e.g.*, *id.*

characterizes cell phones" as well as the quantity and quality of data that they contain in its discussion of just how integral today's smartphones are to modern life, and the various purposes for which they are used.[13] A key challenge for organizations is to find ways to disentangle the personal from the professional when it comes to protecting and monitoring data on their employees' devices—and this premise assumes it is even possible to make a meaningful distinction between the two.

[4] Organizations approach BYOD from different angles, and a variety of factors may influence the internal policies and procedures an organization chooses to implement when it launches an employee BYOD program. Although the term "BYOD" may refer to personal use by employees of employer-owned devices, more typically, BYOD is understood as employee use of a personally-owned device to conduct work activities.[14] Most BYOD policies cover laptop computers as well as mobile phones and tablets, and many employers provide a subsidy to cover the cost of the device, the data plan, or both.[15] BYOD and corporate-owned, personally enabled (or "COPE") strategies may focus on separating workspaces into a "'two devices in one' approach, where each space is configured and managed separately, with distinct policies for connectivity, app permissions, [and] security options."[16] Organizations

[13] *See id.* at 2489–90 ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[14] *See, e.g.*, Press Release, Gartner, Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes (May 1, 2013) [hereinafter Gartner Press Release], http://www.gartner.com/newsroom/id/2466615, *archived at* http://perma.cc/GMN5-CSVQ ("Gartner defines a BYOD strategy as an alternative strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data.").

[15] *See id.*

[16] HETTING, *supra* note 8, at 20.

often deploy BYOD and COPE programs simultaneously, but based on court decisions that implicate mobile devices and related technologies, courts will expect the results of these efforts—especially regarding legal hold preservation—to operate according to the same concept of control regardless of the program or programs the organization chooses.[17] The "two in one" method may bolster security by requiring corporate apps to connect over secure and encrypted VPNs and preventing personal apps from accessing services through the corporate network, but allowing more connectivity options with respect to the personal space on the device.[18]

[5] There are still laggards, organizations that do not directly address their employees' use of personal mobile devices for work purposes. But given rapid advancements in technology and behavioral shifts with respect to mobile device cross-use, it is becoming increasingly difficult for any organization to maintain plausible deniability when it comes to how its corporate data is being stored on devices that are outside of the organization's logistical control.[19] Failing to acknowledge that workers

[17] *See* Richard Absalom, *Beyond BYOD: How Businesses Might COPE with Mobility*, BLACKBERRY 14, http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/Beyond-BYOD-BlackBerry-Ovum.pdf, *archived at* http://perma.cc/YEM8-T2XA (last visited Feb. 13, 2015); *see also* Philip Favro, *Breaking News: Mobile Device Preservation Failures Lead to Doomsday eDiscovery Sanctions*, MIND OVER MATTERS (Sept. 11, 2014), http://www.recommind.com/blog/breaking-news-mobile-device-preservation-failures-lead-doomsday-ediscovery-sanctions, *archived at* http://perma.cc/2WK5-M369.

[18] HETTING, *supra* note 8, at 20–21.

[19] *See* BRING YOUR OWN DEVICE—SECURITY AND RISK CONSIDERATIONS FOR YOUR MOBILE DEVICE PROGRAM 5 (Ernst & Young 2013) [hereinafter BRING YOUR OWN DEVICE], *available at* http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf, *archived at* http://perma.cc/EW92-NGD3 ("In the US, end users feel an increased sense of ownership of the devices they use at work, and would like to retain as much control as possible. This often includes a sense of entitlement to unlock, 'root' or 'jailbreak' the operating system of the device, and thereby removing many of the operating system's security features and introducing security vulnerabilities. The sense of ownership may also cause the user to be less inclined to immediately notify the organization of device loss.").

are using business devices for personal purposes and vice-versa (or both at the same time) is a dangerous proposition.[20] Data security breaches triggered by the loss of mobile devices; spoliation instructions or other sanctions in litigation; reputational harm; damage to client relationships; and even corporate espionage[21]—these are just a handful of the serious consequences of taking a less-than-rigorous approach to the management of BYOD issues within an organization. But the benefits of well-managed BYOD programs to both employers and employees seem to be pushing the marketplace inexorably toward BYOD ubiquity.[22]

[6] Although civil suits and other legal and regulatory challenges related to mobile device policies are proliferating in the United States, at this time there are no federal or state statutes that specifically govern BYOD policies or practices as such. International jurisdictions, collectively and individually, present their own difficulties—not so much in terms of specific barriers to BYOD programs, but rather in the dearth of clear, applicable guidelines for compliant implementation. Unsurprisingly, this disjointed legal and regulatory landscape is difficult for organizations to navigate, and practical solutions are scarce. That said, in this paper we will present a "lay of the land" with respect to BYOD implementation in the United States and Europe by discussing current technologies and practices and providing an overview of existing laws and guidelines that may apply to BYOD programs. Relevant issues will be presented in the form of hypothetical situations encountered by a fictitious globetrotting employee whose typical activities serve to highlight the legal challenges and complexities inherent in doing digital business across

[20] *See, e.g.*, Hammerquist, *supra* note 6. These uses may be more quotidian than often remarked; some authors focus on the not-uncommon use of "personal thumb drives to facilitate working from home on personal computers" which certainly qualify as BYOD. *See id.*

[21] *See id.*

[22] *See, e.g.*, Gina Smith, *10 Myths of BYOD in the Enterprise*, TECHREPUBLIC (Feb. 16, 2012 5:50 AM), http://www.techrepublic.com/blog/10-things/10-myths-of-byod-in-the-enterprise/, *archived at* http://perma.cc/Q2D6-C9MU.

borders. We will conclude by offering a checklist of considerations that organizations may use to help guide the development of a nascent BYOD program, or to evaluate the compliance posture of current BYOD policies and practices.

II. OVERVIEW: CASE STUDY

[7] *Our hypothetical employee, Julie Jetset, manages global IT forensic investigations for a U.S.-based multinational consulting company we'll call Omniscient Everywhere, Inc. ("OEI"). Julie is a dual citizen of the United States and France, and has a desk in OEI's New York and Paris offices, though the nature of her client engagements often has her traveling to three other countries in as many days. Julie's primary job responsibilities include meeting on-site with OEI clients; managing a team of highly-skilled technologists (who are based in seven different countries); and running in-depth investigations of sophisticated data security incidents. Julie has signed a number of policies regarding the acceptable use of OEI systems and networks, and OEI data in her possession has been subject to a litigation hold on more than one occasion.*

[8] For the most part, managing BYOD issues is viewed as the employer's responsibility. But individual employees like Julie also play a part—whether they are aware of the risks[23] or not.[24] Organizations face a variety of legal challenges with respect to employees who live and work in multiple jurisdictions. In addition to the traditional complexities of immigration status, work permits, employment contracts, payroll taxes, and local labor codes,[25] a host of new challenges have arisen with the

[23] *See* BRING YOUR OWN DEVICE, *supra* note 19, at 5.

[24] *See, e.g.*, Amanuel Tsighe, *Minimizing Insider Threats: The Unwitting Disclosure*, FILEOPEN (Oct. 2013), http://www.fileopen.com/blog/archive/2013/10, *archived at* http://perma.cc/JM7J-C9H8.

[25] *See* Kevin Cranman & Natasha Baker, *Where in the World Are Your Employees? Institutions as Global Employers: Employment Law Considerations in the Age of International Programs*, 36 J.C. & U.L. 565, 571 (2010).

increased use of mobile computing devices and heightened attention to data protection issues.[26] Confidentiality has always been on the corporate radar, but electronic data security and data protection law compliance are demanding an increasingly significant amount of attention. For example, when workers are operating in countries that have omnibus data protection laws with restrictions on cross-border transfers of personal data, organizations may need to register their employees' data processing activities with local authorities or establish a data transfer mechanism to allow the employees to carry out their job functions in a compliant manner.[27]

[9] Julie's mobile device usage implicates both issues: how stored data travels with Julie from country to country, as well as how the data travels to and from Julie's devices as it instantaneously traverses borders, switches carriers and methods of transfer,[28] and is stored momentarily, or permanently,[29] as it continues on its way.[30]

---

[26] *See, e.g.*, William Long, *BYOD: Data Protection and Information Security Issues*, COMPUTERWEEKLY (Oct. 11, 2013), http://www.computerweekly.com/opinion/BYOD-data-protection-and-information-security-issues?vgnextfmt=print, *archived at* http://perma.cc/DV7G-Q76R.

[27] *See, e.g.*, Donald C. Dowling, Jr., *Cross-Border Telecommuting Checklist*, JDSUPRABUS. ADVISOR (Nov. 4, 2013), http://www.jdsupra.com/legalnews/global-hr-hot-topicnovember-2013-cross-66155/, *archived at* http://perma.cc/RW97-67AD.

[28] Methods of transfer may include simple disc or flash transfers, or a number of different wireless technologies (e.g., cellular, WiFi, Bluetooth, Infrared, and WiMAX). *See* T. Sridhar, *Wi-Fi, Bluetooth and WiMAX*, 11 THE INTERNET PROTOCOL J. 4 (Dec. 2008), *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_11-4/114_wifi.html, *archived at* http://perma.cc/5NEJ-9ARM.

[29] *See* Melissa Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U.L. REV. 267, 273 (2013) ("For webmail users, the computer or mobile device merely serves as a conduit to access the remote server . . . ").

[30] *See* Brian Dougherty et al., *Overcoming Cellular Connectivity Limitations with M2Blue Autonomic Distributed Data Caching*, 35 CSI COMMC'NS 16, 17–18, (Aug. 2011), *available at* http://csi-india.org/c/document_library/get_file?uuid=444ae842-

III. CURRENT STATE OF TECHNOLOGY AND USAGE

[10] *Julie still has an OEI-issued Blackberry she keeps as a backup, but she usually works on either the iPhone she purchased that segregates her OEI e-mail and applications from her personal apps and data, or on her iPad (on which she mirrors her OEI e-mail). Julie also uses an Android tablet to run OEI-specific forensic tools and human resource management software, as well as certain otherwise-unsupported proprietary programs that are used in her team's technical investigations. Because of her travel and an expectation of constant availability, OEI pays for Julie's data and cellphone usage.*

[11] Are corporate BYOD policies enough to prevent improper use by employees, or at least to shield an organization from liability in the event improper use results in actionable harm? Or is this type of technology simply at odds with current or future legal requirements? Are BYOD programs doomed to fail, to be replaced with a return to employer-chosen devices as the default practice? As is often the case in the e-Discovery context, perfection is not the appropriate standard to apply in a world of myriad technological possibilities.[31] Taking an approach that focuses on pragmatic policies and procedures that hew to the spirit of the relevant regulations is, perhaps, the most rational path forward when strict compliance with every rule and judicial decision could lead to illogical, even conflicting, extremes. Julie's global BYOD use may be artificially exaggerated for illustrative purposes, but her situation is not an exception to the rule. These types of issues are only growing in number and complexity, and, by and large, organizations and lawmakers are not leading by policy or example—they are instead scrambling to keep up.

7538-4111-a09c-1daefee5c2dc&groupId-10157, *archived at* http://perma.cc/GYC2-F6AX.

[31] *See* Craig B. Shaffer, *"Defensible" By What Standard?*, THE SEDONA CONFERENCE 3 (2012) (citing *The Sedona Conference Commentary on Achieving Equality in the E-Discovery Process*, 10 SEDONA CONFERENCE J. 299, 307 (Fall 2009)), *available at* http://thesedonaconference.org/system/files/LR_Defensible_by_what_standard.pdf, *archived at* http://perma.cc/YUV5-ZPVU (automatic download).

A. BYOD Today

[12] By all accounts, the implementation of BYOD programs in the United States is on the rise and shows no signs of slowing down. In 2013, Gartner predicted that by 2017 half of employers would require employees to supply their own mobile devices for work purposes.[32] Throughout most of history, this would represent a rather staggering shift over a very short period of time, but mobile and mobile-related growth rates[33] have their own unique math and exponential growth curves.[34] This trend may actually accelerate if other courts follow the example of a recent California state court decision that found employers are required to pick up the tab for work-related calls made on personal cell phones.[35] The Gartner study also found that BYOD programs are most common in medium to large organizations (defined as those with revenues of $500 million to $5 billion and 2,500–5,000 employees), but noted that companies in the United States are twice as likely as their European counterparts to adopt BYOD models.[36] Although study data from 2013 projected modest BYOD device adoption growth rates of only "between

[32] *See* Gartner Press Release, *supra* note 14.

[33] *See Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019*, 1, 3–4, 17–20 (2015), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf, *archived at* http://perma.cc/B9XF-5SMK.

[34] *See, e.g.*, Liz Gannes, *Meeker: As Internet User Growth Slows, the Real Driver Is Mobile Usage*, RE/CODE (May 28, 2014 8:05 AM), http://recode.net/2014/05/28/meeker-as-internet-user-growth-slows-the-real-driver-is-mobile-usage/, *archived at* http://perma.cc/CQ62-CQKY.

[35] *See* Cochran v. Schwan's Home Serv., Inc., 228 Cal. App. 4th 1137, 1143–44 (2014) (noting although this decision concerned a specific provision of California's Labor Code, commentators indicate both that similar suits in other states may be successful on the same grounds, and that such holdings likely would be extended to apply to data charges as well).

[36] Gartner Press Release, *supra* note 12.

15 percent and 38 percent in the major markets,"[37] the more relevant consideration may be the fact that mobile data traffic is exploding, with growth rates topping 80%.[38]

[13] The United States currently leads the pack with respect to BYOD device adoption, but "China . . . [and] India . . . [are] not far behind."[39] A 2013 consumer research study of workers in seven major economies demonstrated a higher prevalence of standard mobile device or smartphone use in China and India (as compared to desktop and laptop computer usage).[40] In both countries, more than three-quarters of the respondents indicated that they use standard mobile devices or smartphones.[41]

[14] According to an Avanade Singapore study conducted in early 2013

> 72 percent of organizations in Asia-Pacific said the majority of their employees use personal computing devices in the workplace . . . higher than the global average of 61 percent . . . 72 percent of respondents from both Singapore and Malaysia said their employees bring their own devices to work while 61 percent of Australian organizations do so.[42]

[37] *See* HETTING, *supra* note 8, at 4.

[38] *See* Gannes, *supra* note 34.

[39] HETTING, *supra* note 8.

[40] *See* DAVID A. WILLIS, BRING YOUR OWN DEVICE: THE FACTS AND THE FUTURE, 9–10 (Gartner 2013), *available at* https://l1.osdimg.com/remote-support/dam/pdf/en/bring-your-own-device-the-facts-and-the-future.pdf, *archived at* https://perma.cc/X926-6ZYM.

[41] *See id.* at 10.

[42] Liau Yun Qing, *BYOD on Rise in Asia, but Challenges Remain*, ZDNET (Feb. 4, 2013 2:23 AM), http://www.zdnet.com/article/byod-on-rise-in-Asia-but-challenges-remain/, *archived at* http://perma.cc/8C5T-U4D7.

A broad-based BYOD survey conducted in late 2012 gathered responses from 3,796 consumers across 17 different countries.[43] When broken down by market, a well-defined trend is noticeable: respondents in the emerging, "high-growth" markets (including Brazil, Russia, India, United Arab Emirates, Malaysia, Singapore, and South Africa) demonstrate a much greater propensity to use their own device at work.[44] Almost 75% of users in these countries did so, in contrast to only 44% in the more mature, developed markets (including Japan, Australia, Belgium, France, Germany, Italy, Spain, Sweden, the UK, and the U.S.).[45]

[15] The stronger preference for BYOD among full-time employees in emerging markets is indicative of several influencing factors.[46] First, organizations in these countries are less likely to provide company-owned mobile handsets or tablets, leaving employees little choice but to use their personal devices.[47] Second, it appears that employees in high-growth emerging markets are more comfortable blurring the boundary between work and personal life than employees in more mature markets.[48] In other words, employees in places like Brazil, South Africa, and Malaysia are thought to have more flexible attitudes to working hours, and are willing to use their own devices to get the job done where necessary.[49] Third, in

[43] *See* ADRIAN DRURY & RICHARD ABSALOM, BYOD: AN EMERGING MARKET TREND IN MORE WAYS THAN ONE 1 (Ovum 2012), *available at* http://www.us.logicalis.com/globalassets/united-states/whitepapers/logicalisbyodwhitepaperovum.pdf, *archived at* http://perma.cc/26ZQ-XYZR (choosing selection criteria for taking the survey only required that these individuals had to be full-time employees in organizations with more than 50 employees).

[44] *See id.* at 2.

[45] *See id.*

[46] *See id.* at 3.

[47] *See id.*

[48] *See id.* at 3.

[49] *See* Drury & Absalom, *supra* note 43, at 3.

less consumer-driven economies, there appears to be a stronger tendency among professionals toward putting work life ahead of personal life; employees are more willing to "live to work" rather than viewing work as a means to fund their lifestyles.[50]

[16] Of course, some outliers exist. For instance, in Spain 62.8% of employees—well above the developed market mean of 44.4%—bring their own device to work.[51] This deviation could be linked to the struggling Spanish economy (i.e., workers are willing to go further to get ahead in their jobs, because losing them would be potentially disastrous given high unemployment rates)[52] or there may be other cultural or demographic factors at play.

[17] In mature markets such as France—where BYOD rates are lowest (30.9%)—"employees are demonstrating an ingrained set of behaviors that demands clear separation of work and personal time, and a much lower level of comfort with the blurring of professional and work life."[53] In addition to the aforementioned "work to live" attitude, resistance to BYOD also reflects a focus on privacy and the desire to keep personal activities secret from any type of authority—whether from the state or an employer.[54] As one study notes

> Europeans in particular have been fiercely protective of their privacy rights given the regional history of authoritarian governments monitoring and censoring personal communications. Elsewhere, attitudes are different: in countries such as the US . . . privacy is largely a secondary issue [to other concerns such as freedom of

[50] *Id.*

[51] *Id.*

[52] *See id.*

[53] *Id.*

[54] *See id.*

> speech or self-determination]; in others, where censorship is either ongoing or where the memory is much more recent, such as Brazil or Russia, the prevailing attitude is that authorities can always see what you are doing anyway—so it doesn't matter who owns the device you use for either work or personal purposes.[55]

[18] In Europe, there are few formal programs in place, and BYOD still tends to happen "off the book[s]."[56] Recent data demonstrates that only about 30% of Continental European organizations maintain formal BYOD policies,[57] with UK organizations slightly higher at 48%.[58] Unlike in the United States, where BYOD continues to trend upward, it seems BYOD uptake among organizations in Europe has been relatively static.[59]

[19] This stagnation may be attributed to cultural differences. For example, in Europe there exists a "cultural expectation that your employer will provide you with the tools to do your job" so employees may resist the idea of paying for devices that will be used for work purposes.[60] It is interesting to note that

---

[55] Drury & Absalom, *supra* note 43, at 3.

[56] Stuart Lauchlan, *BYOD or CYOD—An International Divide Across the Pond?*, DIGINOMICA 2 (Jan. 3, 2014), http://diginomica.com/2014/01/03/byod-cyod-international-divide-pond/, *archived at* http://perma.cc/DL5T-676Z.

[57] *See* Jane McCallion, *BYOD More Popular in US than Europe, Says IDC*, PCPRO (Jun. 4, 2014), http://www.pcpro.co.uk/news/enterprise/389131/byod-more-popular-in-the-us-than-europe-says-idc, *archived at* http://perma.cc/JU7P-VZB9.

[58] *See* Andy McCue, *Has the BYOD Bubble Burst?*, FUTURE THINKING, http://futurethinking.ee.co.uk/has-the-byod-bubble-burst/, *archived at* http://perma.cc/57X8-PJ5C (last visited Feb. 27, 2015).

[59] *See, e.g.*, McCallion, *supra* note 57.

[60] Tom Kaneshige, *CIOs in Europe Say BYOD is Stalling*, CIO, (Jul. 23, 2014 1:53 PM), http://www.cio.com/article/2457446/byod/cios-in-europe-say-byod-is-stalling.html, *archived at* http://perma.cc/4MJF-8NYX.

> In fact, only 6% of European employees are willing to pay for a mobile/smartphone used for work in full, while 18% are willing to make a contribution. The willingness to pay is lower with tablets: Only 4% of respondents happily pay for it in full, and 15% willingly contribute to it.[61]

Employees in Europe also tend to shy away from BYOD programs because they are reluctant to sign away their expectations of privacy.[62]

[20] Research points to six major "euro barriers" to successful BYOD adoption on the continent: (1) prohibitively high cross-border data roaming costs; (2) legislation regulating employees, such as national health and safety rules; (3) employee data protection laws that prevent data security enforcement because personal devices are considered the employee's private property; (4) European tax and labor laws that inhibit allowances for mobile contracts and applications (unlike in the United States where such reimbursement is common practice); (5) responsibility for device security is shouldered by employees who participate, forcing executives to understand and manage risks, such as those associated with upgrades; and (6) private devices cannot easily be supported by corporate help desks, which in turn jeopardizes business continuity.[63]

[21] European organizations also tend to see BYOD programs as prohibitively expensive.[64] For instance, the BBC's head of IT and strategy said in 2013 that "providing staff with £500 (USD 750) to buy a device to use at work would cost an organization £700 (USD 1050), while the

[61] Lauchlan, *supra* note 56.

[62] *See* Kaneshige, *supra* note 60.

[63] *See* Lauchlan, *supra* note 56.

[64] *See, e.g.*, Nick Heath, *Is BYOD Here to Stay? Maybe it's Just a Phase You're Going Through*, (June 5, 2014 2:31 AM), http://www.techrepublic.com/blog/european-technology/is-byod-here-to-stay-maybe-its-just-a-phase-youre-going-through/, *archived at* http://perma.cc/5MRG-WQDV.

individual would only get £300 (USD 350) worth of benefit."[65] The organization would face costs associated with "tax liabilities, higher tariffs on consumer data and voice plans and subscription payments for third-party mobile device management software."[66]

[22] Confronted with the challenges and expenses associated with implementing BYOD programs in Europe, many organizations are looking at viable alternatives including a "choose your own device" ("CYOD") option.[67] With CYOD policies, employees are able to select from a list of organization-supported devices and applications.[68] In contrast to BYOD, in CYOD policies the "devices are funded, supplied, and fully managed by the organization."[69] However, CYOD policies may require some organizational flexibility, such as allowing limited private usage to foster employee satisfaction.[70]

[23] Research regarding the Australian market indicates businesses there also may be shifting toward CYOD policies.[71] Australian organizations have been frustrated by the "complexity of delivering, managing, and supporting mobile applications" on a host of employee-owned devices.[72] CYOD facilitates these processes for IT departments by

[65] *Id.*

[66] *Id.*

[67] Lauchlan, *supra* note 56.

[68] *See id.*

[69] *Id.*

[70] *Id.*

[71] *See, e.g.*, Press Release, IDC, Australian ICT Growth Driven by 3rd Platform Technologies, According to IDC (Feb. 6, 2014), *available at* http://www.idc.com/getdoc.jsp?containerId=prAU24666014, *archived at* http://perma.cc/VDV9-5VQJ.

[72] *Id.*

allowing them to "limit the number of devices, form factors, and operating systems."[73]

[24] Unfortunately for those who would prefer that European and Australian preferences dominate the BYOD landscape, lower BYOD adoption rates reduce pressure to establish standards for organizations to follow as best or defensible practices. In turn, this makes it more likely the U.S. and the developing world will lead by market force, establishing common BYOD practices that may conflict with European privacy sensibilities and concerns. To imagine how this might play out in practice, we need only look at the 2010 United States Department of Justice materials that describe how some of the major U.S. cellular carriers collected and retained various kinds of information on consumer usage.[74] The data included subscriber information (replete with personally identifiable information), call detail records, cell towers used by the device (essentially geolocation), text message detail and content, pictures, and IP session with destination information (which websites or other applications the user accessed, and for how long).[75]

B. Employee Behavior

[25] Not only are BYOD devices full of personal information, they also present security risks associated with the "end node problem"[76] which presents when an employee's device is used to access both highly secured

[73] *Id.*

[74] *See* U.S. Dep't of Justice, *Retention Periods of Major Cellular Service Providers* (Aug. 2010), https://www.aclu.org/files/pdfs/freespeech/retention_periods_of_major_cellular_service_providers.pdf, *archived at* https://perma.cc/MX8F-9SDD.

[75] *See id.*

[76] Stuart Errington, *BYOC/BYOD—What is it?* BOWKERIT, http://www.bowkerit.co.uk/news_more.asp?news_id=28&current_id=1, *archived at* http://perma.cc/7B7E-BUNE (last visited Feb. 27, 2015).

as well as unsecured networks, and data is exchanged across both types of barriers.[77] This cross-usage creates a scenario in which a device may become infected with malware while off the corporate network, and then spread the malware to the organization when the user reconnects to the employer's system.[78] These types of concerns arise for organizations when the purchaser, primary user, and device maintainer of a BYOD device are all the same person: the employee.

[26] Personal use of employer-owned technology at work has been the normal course of business for quite some time, as has been recognized by courts and commentators alike.[79] But one "oft-overlooked security threat is the practice of employees lending BYOD devices to friends and family in an unlocked state [which may] leak more sensitive information than malicious attacks by hackers."[80] It is through these small gaps that an otherwise solid foundation may begin to crack. And even if various individual instances of non-compliance do not result in harm or lead to legally-cognizable security breaches, implementing BYOD programs that restrict user behavior in certain ways has the potential to trigger "employee-employer (and even trade union) disputes resulting in divisive

[77] *See* Woodworth, *supra* note 1, at 8.

[78] *See* HETTING, *supra* note 8, at 9.

[79] *See* City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("[M]any employers expect or at least tolerate personal use of [electronic communications] equipment by employees because it often increases worker efficiency."); *see also* NLRB, Board Decision, Purple Commc'ns, 361 N.L.R.B. No. 126, 201 L.R.R.M. (BNA) 1929, 2014–2015 NLRB Dec. (CCH) ¶ 15,890, 2014 NLRB LEXIS 952, at *30 (Dec. 11, 2014); R. Sprague, *Employee Electronic Communications in a Boundaryless World*, 53 U. LOUISVILLE L. REV. (forthcoming 2015) (manuscript at 1–3), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2510919, *archived at* http://perma.cc/3QZ7-BKWF.

[80] HETTING, *supra* note 8, at 7 (citing FIN. CRIMES ENFORCEMENT NETWORK, IDENTITY THEFT: TRENDS, PATTERNS, AND TYPOLOGIES REPORTED IN SUSPICIOUS ACTIVITY REPORTS 4 (Oct. 2010), *available at* http://www.fincen.gov/news_room/rp/reports/pdf/ID%20Theft.pdf, *archived at* http://perma.cc/CYD3-7KEM).

litigation."[81]

C. Device Security Management vs. Employee Personal Data

[27] So-called Enterprise Mobility Management ("EMM") programs can provide physical security on employee devices through the use of device passwords, workspace passwords, "hardware-level encryption of (at least) all corporate data" on the device, and centralized password management "with features for strength, length, time validity, and minimum complexity." [82] Mobile Device Management Solutions ("MDMs") may "grant the ability to lock and wipe devices that have access to the network" but may also "back up data, monitor traffic, [and] manage applications stored on devices."[83] Establishing a metaphorical "'locker' of sorts for the secure storage of work related data and files,"[84] this type of solution may be too involved for less sophisticated organizations. A "lighter touch" with respect to this type of technology may provide the option to "segment company from personal data, keeping the employee's own information private."[85] The locality may matter, however, since it is illegal for an employer to wipe a device it does not own in certain countries, including France and Italy.[86]

---

[81] *ABA Criminal Justice Section Presents: Collision Course Ahead? Personal Data Privacy vs. Corporate Security in a BYOD World*, A.B.A. (Aug. 8, 2014), http://www.americanbar.org/content/dam/aba/events/criminal_justice/BYOD.authcheckdam.pdf, *archived at* http://perma.cc/2568-63F9.

[82] HETTING, *supra* note 8, at 19.

[83] Woodworth, *supra* note 1, at 14.

[84] Peter F. McLaughlin, *BYOD: Cool but Dangerous—3 HIPAA Security Rule Challenges, 7 Key Precautions*, DLA PIPER (Sept. 24, 2014), https://www.dlapiper.com/en/us/insights/publications/2014/09/bring-our-own-device/, *archived at* https://perma.cc/V2QP-8PHD.

[85] Erik Hammerquist, *Vendor Voice: BYOD Is the No. 1 E-Discovery Challenge for 2014*, L. TECH. NEWS, Jan. 16, 2014.

[86] HETTING, *supra* note 8, at 12.

[28] As reported by the Wall Street Journal, erasures of employee-owned devices are on the rise, with statistics from one MDM firm indicating that it had wiped 81,000 devices in the first six months of 2014 (as compared to only 51,000 in the second half of 2013).[87] About half of the device erasures over a 13-month period ending in June 2014 were "auto-deletes" that were triggered by an established policy responding to events such as a data security breach or the theft of a device.[88] The rest of the deletions were conducted manually by IT personnel, usually at the time of employee separation and on the request of the human resources department.[89] As discussed further below, the remote wiping of a device for security purposes may cause an employee to unexpectedly lose valuable personal data. In some cases, such losses have resulted in litigation.

IV. EXISTING STATUTORY AND COMMON LAW APPLICABLE TO BYOD

A. United States

[29] When it comes to monitoring employee activities electronically in the United States, organizations "have few legal obligations other than informing employees."[90] A raft of new surveillance tools holds the promise of increasing worker productivity and helping businesses fine-tune their workforce management strategies, but the "specter of unchecked

[87] *See* Lauren Weber, *Every Three Minutes, a Worker's Personal Device Is Remotely Wiped*, WALL ST. J. (Sept. 8, 2014, 10:20 AM), http://blogs.wsj.com/atwork/2014/09/08/every-three-minutes-a-workers-personal-device-is-remotely-wiped/, *archived at* http://perma.cc/YZ2G-696X.

[88] *See id.*

[89] *See id.*

[90] Steve Lohr, *Unblinking Eyes Track Employees*, N.Y. TIMES, June 21, 2014, at A1, *available at* http://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html, *archived at* http://perma.cc/VEP3-JG4K.

surveillance" by employers has privacy advocates concerned.[91] Among the various tracking methods available to organizations, the ability to monitor employees through their mobile devices may offer the most robust—and useful—data, but it also poses the greatest risks to privacy.

[30] Although there are no federal or state laws that expressly apply to BYOD policies or practices as such, certain federal electronic monitoring statutes may be relevant to employer access to employee information transmitted by—or stored on—BYOD devices: the Electronic Communications Privacy Act;[92] the Stored Communications Act;[93] and the Computer Fraud and Abuse Act.[94] That said, at least one commentator has characterized a properly implemented BYOD policy as promoting an invasion of privacy, stating such a policy would "destroy[] essential elements of the Wiretapping Act [and] [t]he Stored Communications Act."[95]

1. The Electronic Communications Privacy Act ("ECPA") and Employee Expectations of Privacy

[31] In the United States, courts have tackled the question of what constitutes a "reasonable expectation of privacy" for Fourth Amendment protection purposes many times over the years, including with respect to privacy expectations in the workplace.[96] An individual's right to privacy

[91] *Id.*

[92] Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C. & 47 U.S.C.).

[93] Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2712 (2012).

[94] Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2012).

[95] Woodworth, *supra* note 1, at 30.

[96] *See, e.g.*, Katz v. U.S., 389 U.S. 347, 351–52 (1967) ("[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally

depends largely on context and a fact-specific inquiry, but generally is determined with reference to the two-prong test outlined in Justice Douglas's concurrence in *Katz v. U.S.*: (1) does the person have an "actual (subjective) expectation of privacy"; and (2) is that expectation of privacy "one that society is prepared to recognize as 'reasonable.'"[97] More recent decisions in this vein have highlighted how the ubiquitous use of rapidly-developing new technologies has both dramatically expanded the variety of scenarios in which an individual's privacy might be invaded, and opened brand new avenues of discussion regarding what constitutes a "reasonable" expectation of privacy.[98] Although the ECPA ostensibly would protect the privacy of employee communications vis-à-vis their employers, exceptions to the ECPA effectively allow employers to intercept or access such communications if the employee at issue has consented to a privacy policy regarding employer access,[99] or if the communication relates to the business and the interception is necessary to protect the company's interests.[100]

protected." (citations omitted)); O'Connor v. Ortega, 480 U.S. 709, 717 (1987) ("We reject the contention . . . that public employees can never have a reasonable expectation of privacy in their place of work. Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."). *But see, e.g.*, Cal. v. Ciraolo, 476 U.S. 207, 213 (1986) ("That the area is within the curtilage does not itself bar all police observation. The Fourth Amendment protection of the home has never extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible.").

[97] *Katz*, 389 U.S. at 361 (Douglas, J., concurring).

[98] *See, e.g.*, U.S. v. Jones, 132 S. Ct. 945, 948 (2012) (discussing whether attaching a Global-Positioning-System (GPS) tracking device to an individual's car is a search or seizure within the meaning of the Fourth Amendment).

[99] *See* 18 U.S.C. § 2511(2)(c)–(d) (2012).

[100] *See id.* at § 2511(2)(a)(i).

[32] But an organization may be limited in its ability to obtain consent to access personal, private information, even on company-issued devices. In *Stengart v. Loving Care Agency, Inc*., the New Jersey Supreme Court stated that an employer did not have the right to review all information contained on an employee's company-issued device, finding that "a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications . . . would not be enforceable."[101] But other jurisdictions have found otherwise, holding that there may be no expectation of privacy in company computers,[102] and allowing employer access policies to be implemented through tacit consent and "pop-up" windows (on employer-owned devices).[103]

[33] Further distinctions may be made with respect to the ownership of the device and the purposes for which the device is used. For example, some courts are still articulating a distinction between personal and business e-mail accounts.[104] And certain perceived invasions of employee privacy also may give rise to a common law tort claim, such as a claim for "intrusion upon seclusion" in situations where "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[105]

---

[101] Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 665 (N.J. 2010).

[102] *See* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002).

[103] *See* Sporer v. UAL Corp., No. C 08-02835 JSWf, 2009 U.S. Dist. LEXIS 76852, at *16–17 (N.D. Cal. 2009).

[104] *See In re* Info. Mgmt. Servs., Inc. Derivative Litig., 81 A.3d 278, 285 n.1 (Del. Ch. 2013) (holding "[a] work e[-]mail account differs from a personal, password-protected, web-based e[-]mail account, also known as webmail, which the employee may obtain through Google, Hotmail, or other services" and stating "[c]ourts have generally afforded greater privacy protection to webmail and have reached divergent conclusions when analyzing the attorney-client privilege if the employee and personal attorney communicated using webmail.")

2. The Stored Communications Act

[34] The Stored Communications Act ("SCA") aims to protect electronic communications in the United States by (1) providing a private cause of action against anyone who "intentionally 'obtains, alters, or prevents authorized access' to certain stored communications;" (2) regulating when network service providers may voluntarily disclose customer communications and records; and (3) outlining specific rules that govern when state actors "may compel disclosure of stored communications from network service providers."[106] In response to legal uncertainty associated with a perceived gap between the Wiretap Act and the Fourth Amendment, Congress passed the SCA in an attempt to create a balance between a public right to privacy, continuing technological progress, and effective, legitimate law enforcement.[107]

[35] It is difficult, however, to apply the SCA in the face of changing technologies. For example, in *Theofel v. Farey-Jones*, contrary to traditional interpretation of the SCA, the Ninth Circuit determined that post-transmission e-mails held by the service provider qualified as "electronic storage" and were therefore covered by the SCA's protections.[108] Despite dicta to the contrary in *Theofel*, this logic was extended in *Quon v. Arch Wireless Operating Co.*, and the *Quon* court

[105] RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see, e.g.*, Sitton v. Print Direction, Inc., 718 S.E.2d 532, 534, 537 (Ga. Ct. App. 2011) (court declined to find a common law invasion of privacy when employer read e-mails from employee's computer).

[106] *See* Medina, *supra* note 29, at 277.

[107] *See ECPA (Part I): Lawful Access to Stored Content: Hearing before the Subcomm. On Crime, Terrorism, Homeland Sec., and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 4 (2013) (statement of Rep. Bob Goodlatte, H. Comm. On Judiciary), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg80065/pdf/CHRG-113hhrg80065.pdf, *archived at* http://perma.cc/5Y76-SQGR; *see also* Medina, *supra* note 29, at 276.

[108] *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2004).

found that permanently archived text messages also qualified as storage or "backup."[109]

[36] The recent *Sunbelt Rentals, Inc. v. Victor* decision drew a different distinction when the court held text messages on workplace mobile devices are not protected by the SCA.[110] That decision may have turned on the intricate fact pattern, as Victor had linked his Apple account to his former and future employers' IT environments, electronically tethering the two devices.[111] Facts drive these decisions, as should be evident by comparison with *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, L.L.C.*, in which the court held that the SCA *could* be used against an employer that had implemented a BYOD regime.[112] In that case, the former employee had accessed his Hotmail account at work and left the website such that the "username and password fields were automatically populated."[113] Using the former employee's Hotmail account, a supervisor uncovered Victor's Gmail account username and password, as well as another account based on a "lucky guess" related to a password the former employee used elsewhere.[114] The supervisor's activity resulted in the former employee winning summary judgment on his SCA claim against Pure Power.[115] The difference between *Sunbelt* and *Pure Power* might simply have been that the Pure Power supervisor intentionally tried to force a connection using the former employee's access to a personal account. It is also possible that the automatic operation and linking

[109] *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902–03 (9th Cir. 2008).

[110] *See* Sunbelt Rentals, Inc. v. Victor, No. C 13-4240 SBA, 2014 U.S. Dist. LEXIS 121039, at *19–21 (N.D. Cal. Aug. 28, 2014).

[111] *See id.* at 20–21.

[112] Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, L.L.C., 587 F. Supp. 2d 548, 555–56 (S.D.N.Y. 2008).

[113] *Id.* at 552.

[114] *Id.*

[115] *Id.* at 419.

between Victor's accounts—a practice touted by Apple as a selling point [116] and something Sunbelt simply had no prior warning of—distinguishes the cases.

3. The Computer Fraud and Abuse Act ("CFAA")

[37] The CFAA started out as a means to protect government computers against hackers, [117] but over the years has been applied to cover unauthorized access by employees when they act against their employers' interests. [118] As currently construed, at least by the United States government, the CFAA covers seven types of activities: (1) obtaining national security information; (2) compromising the confidentiality of a computer; (3) trespassing in a Government computer; (4) accessing a computer to defraud and obtain value; (5) transmission or access that causes damage; (6) trafficking in passwords; and (7) extortion involving threats to damage a computer.[119] Even though those categories may seem stacked *against* users, read plainly, the CFAA can work both ways, as it defines loss as "any reasonable cost to *any* victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential

[116] *See iCloud—Learn How to Set Up iCloud on All Your Devices.*, APPLE, https://www.apple.com/icloud/setup/ios.html (last visited Feb. 13, 2015) ("Turn on iCloud. . . . Enable automatic downloads. . . . Turn on iCloud for the rest of your devices. To get the most out of iCloud, set it up everywhere.").

[117] *See* Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act : Narrowing The Scope*, 2010 DUKE L. & TECH. REV. 012, ¶ 24 (2010), *available at* http://dltr.law.duke.edu/2010/08/26/disloyal-computer-use-and-the-computer-fraud-and-abuse-act-narrowing-the-scope/, *archived at* http://perma.cc/4N9J-7S4S.

[118] *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006).

[119] *See* H. MARSHALL JARRETT ET AL., U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 3 (n.d.), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf, *archived at* http://perma.cc/4LNK-W5X9.

damages incurred because of interruption of service."[120]

[38] Despite the availability of a right of action—and specific instruction on this point from the government[121]—employees may have difficulty asserting a viable CFAA claim with respect to any personal data lost if their device is wiped by their employer. CFAA claims are cognizable only if the plaintiff can show that the unauthorized access to his or her computer resulted in a loss of at least $5,000 in a one-year period.[122] In *Rajaee v. Design Tech Homes, Ltd.*, former employee plaintiff Rajaee brought claims under the ECPA, the CFAA, and Texas state law when Design Tech deleted all of the data from his personal iPhone, which he was using on a BYOD basis, and which was connected to Design Tech's Microsoft Exchange server.[123] Rajaee asserted that the value of his deleted photos, contact information, and other data amounted to over $100,000, but the court found that the only losses recognized under the CFAA are expenses associated with investigating the incident or costs incurred as a result of an interruption of service.[124] The CFAA clearly applied to the BYOD device, but the idea of personal data privacy as a cognizable right with associated value played into the court's decision, as it had when the CFAA was drafted.[125] Ultimately, the court found that there was no "cognizable loss" or intrinsic value associated with Rajaee's

[120] 18 U.S.C. § 1030(e)(11) (2012) (emphasis added).

[121] *See id.* at § 1030(g); JARRETT ET AL., *supra* note 119, at 3 ("In some circumstances, the CFAA allows victims who suffer specific types of loss or damage as a result of violations of the Act to bring civil actions against the violators for compensatory damages and injunctive or other equitable relief.").

[122] *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I), (g) (2012).

[123] *See* Rajaee v. Design Tech Homes, Ltd., No. H-13-2517, 2014 U.S. Dist. LEXIS 159180, at *1–3 (S.D. Tex. Nov. 11, 2014).

[124] *See id.* at *5–11 (finding deletion of data does not constitute an "interruption of service" for CFAA purposes).

[125] *See id.*

personal data.[126]

4. e-Discovery Issues

[39] *Julie is investigating a serious network intrusion on-site with a client in Berlin when she receives an e-mail from the OEI Legal Department in New York outlining a new litigation hold. A suit has been filed in federal court in the U.S., seeking damages for financial losses resulting from the intrusion and alleging that OEI's failure to identify the root cause in a timely manner allowed the theft to occur. The litigation is likely to concern diagnostic information Julie has been collecting during the investigation; reports she had been preparing in her Paris office regarding the incident; and log files and other analysis done by members of her team who are physically located in India and in Israel. How can OEI effectively implement this hold? What does Julie need to do to comply?*

[40] In the United States, discovery rules require the preservation and subsequent production of relevant documents based on a concept of "control."[127] However, "'control' does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action."[128] This application requires context; at least one other court has held such custody and control (and the concomitant requirement to preserve and produce) did *not* extend to third-

[126] *See BYOD-Covered Employee Cannot Prove CFAA Loss After Company Remotely Wiped Phone*, 19 ELECTRONIC COM. & L. REP. (BNA) 1488, no. 44 (Nov. 19, 2014) (citing *Rajaee*, 2014 U.S. Dist. LEXIS 159180, at *9–11).

[127] *See, e.g.*, Columbia Pictures Indus. v. Fung, No. CV 06-5578 SVW(JCx), 2007 U.S. Dist. LEXIS 97576, at *3 (C.D. Cal. June 8, 2007) (holding that the party must preserve data within its possession, custody, or control).

[128] Gordon Partners v. Blumenthal (*In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (quoting Bank of N.Y. v. Meridien Biao Bank Tanz. Ltd., 171 F.R.D. 135, 146 (S.D.N.Y. 1997) (citations omitted)).

party consultants, but only to the organization's employees and agents.[129]

[41] These issues are further complicated when employers have policies *against* BYOD, but employees are either ignorant of these polices or intentionally violate them in the performance of their duties.[130] And recent jurisprudence has raised pragmatic questions regarding whether the data is actually under the custody and control of a party who may be nominally—or statutorily—in "control" of the data.[131] But the results must be the same regardless of the practices put in place to with respect to BYOD programs.[132] That is, an organization cannot simply rely upon employees to "do the right thing."

[42] BYOD-related e-Discovery considerations center around two main issues: (1) the argument over whether data is under the "custody and control" of a party; and (2) whether the employer going after—or even asking about—that data implicates the related issue of custodial self-selection. Understandably, employees are often "reluctant to turn over their personal mobile devices for examination."[133] But modern courts have judged parties harshly for devising their own approaches to search

[129] *See* Goodman v. Praxair Servs., 632 F. Supp. 2d 494, 498 (D. Md. 2009).

[130] *See, e.g.*, Woodworth, *supra* note 1, at 5 (citing Press Release, KISS Comm'cns, Bring Your Own Disaster! Warning. BYOD Is Still a Risk for Company Data and Reputation 1, (Oct. 29, 2012), *available at* http://www.sourcewire.com/news/74880/bring-your-own-disaster-warning-byod-is-still-a-risk#.VKyivSvF9EI, *archived at* http://perma.cc/3RUY-8XVD ("almost 80 percent of BYOD activity is inadequately managed by IT departments; nearly half of respondents were either not aware of BYOD activity or ignored its existence, by operating a 'don't ask, don't tell' policy.").

[131] *See, e.g.*, Kickapoo Tribe of Indians v. Nemaha Brown Watershed Joint Dist. No. 7, 294 F.R.D. 610, 614 (D. Kan. 2013) (sustaining an objection, holding that the District could not "compel former members of its Board of Directors, former staff, or former employees to produce documents that are in their possession but are not in the possession of the District itself").

[132] *See* Small v. Univ. Med. Ctr. of S. Nev., No. 2:13-cv-00298-APG-PAL, 2014 U.S. Dist. LEXIS 114406, at *43–46 n. 41 (D. Nev. Aug. 18, 2014).

[133] HETTING, *supra* note 8, at 12.

terms,[134] and collecting certain types of devices from custodians—especially so-called "key players"[135]—may raise the same issues and garner similar scrutiny.

[43] Additional complexity arises where, as "in the text message environment, the ability to save messages, and how many can be saved, is largely device- and carrier-dependent; there is no one answer and certainly no safe 'auto-delete' switch."[136] Even with policies in place, the new reality may be that "each custodian will necessarily undertake the preservation task with varied and potentially incriminating consequences for failure"[137]—particularly where there is no single solution for the issue, or effective uses of EMM "using a multi-[Operating System] BYOD approach may not be an acceptable fit."[138] These new and evolving considerations may undercut earlier guidance that suggested that immediately implementing an MDM to reach out and back up employee devices would comply with related obligations to preserve documents.[139]

[134] *See, e.g.*, *In re* Direct Sw., Inc., No. 08-1984-MLCF-SS, 2009 U.S. Dist. Lexis 69142, at *1–3, 6 (E.D. La. 2009) (ordering defendants to turn over all e-mails concerning the employee plaintiffs, their work, and their hours and the defendants' wage and hour policies and practices after defendants limited the search terms in their query).

[135] *See* Woodworth, *supra* note 1, at 11.

[136] Jonathan M. Redgrave, Keltie Hays Peay & Mathea K.E. Bulander, *Understanding and Contextualizing Precedents in e-Discovery: The Illusion of Stare Decisis and Best Practices to Avoid Reliance on Outdated Guidance*, XX RICH. J.L. & TECH. 8, ¶ 38 (2014), http://jolt.richmond.edu/v20i2/article8.pdf, *archived at* http://perma.cc/2MWM-MSC3.

[137] *Id.*

[138] HETTING, *supra* note 8, at 2.

[139] *See* Woodworth, *supra* note 1, at 16.

5. Federal Trade Commission ("FTC") Guidance on Mobile Privacy

[44] Although not specifically targeted at BYOD programs or employee use of mobile devices, the FTC's Staff Report on mobile privacy disclosures is both relevant and instructive for organizations that provide mobile devices to their employees, or that may monitor employee activity through the employee's mobile device. Issued in February 2013, "Mobile Privacy Disclosures—Building Trust Through Transparency" focused on the rapidly-changing "mobile ecosystem" and the responsibilities of companies acting in the mobile space with respect to consumer privacy issues.[140] The report highlighted the FTC's concerns about how third parties obtain consumer information through mobile devices, how that data may be used or transferred between companies, and most significantly, how details about the collection, use, and sharing of consumer data is relayed to consumers to allow them make informed choices about privacy and security risks associated with their use of mobile technologies.[141]

[45] Because ensuring mobile device security often (if not always) requires organizations to implement some type of MDM solution on employees' devices that store work-related data, the FTC's recommendations almost certainly apply in the BYOD context. For example, the FTC advises mobile platforms or operating system providers to give consumers "just-in-time" notice about data collection activities, and "obtain their affirmative express consent before allowing apps to access sensitive content like geolocation."[142] Ostensibly, this would

[140] *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES—BUILDING TRUST THROUGH TRANSPARENCY i (Feb. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf, *archived at* http://perma.cc/S8VB-JRJ4.

[141] *See id.* at 1.

[142] *Id.* at ii.

include obtaining employee consent for device location tracking, a common feature on company-owned devices to help recover lost devices or remotely wipe the data from those devices to prevent unauthorized access to sensitive information. The FTC also recommended offering a "Do Not Track" option for smartphones, to "allow consumers to choose to prevent tracking . . . as they navigate among apps on their phones."[143] It is unclear exactly how this type of control would function with respect to business-related apps, or whether it would be possible to allow certain limited "tracking" by organizations (e.g., to prevent unauthorized export of company data) while barring surveillance of how employees are using their devices for non-business purposes.

[46] Until the FTC publishes a report providing BYOD-specific guidance, organizations should carefully review the Commission's general recommendations with regard to mobile device privacy and consider their applicability to in-house BYOD policies and procedures.

6. National Institute of Standards and Technology ("NIST") Guidelines

[47] In June 2013, the National Institute of Standards and Technology issued "Guidelines for Managing the Security of Mobile Devices in the Enterprise," a useful tool for organizations working to secure their employees' devices against security threats.[144] The guidelines apply specifically to security concerns that are relevant to BYOD and mobile device use, and "provide[s] recommendations for selecting, implementing, and using centralized management technologies" as well as "securing mobile devices throughout their life cycles."[145] In detailing numerous

[143] *Id.*

[144] *See* MURUGIAH SOUPPAYA & KAREN SCARFONE, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES IN THE ENTERPRISE iii, (spec. publication 800-124, rev. 1, June 2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf, *archived at* http://perma.cc/4LHB-C99W.

[145] *Id.*

strategies and considerations to foster mobile device security improvements, the NIST guidelines focus in on six key recommendations for organizations to implement.[146] First, and perhaps foremost, NIST advises organizations to put in place a thoughtfully-drafted mobile device security policy.[147] In addition, organizations are advised to:

- Develop "system threat models" specific to the organization's mobile devices and the resources that will be accessed through the devices;
- Carefully consider available security services to determine which are appropriate to the needs of the organization, then acquire "one or more solutions that collectively provide the necessary services;"
- Run a pilot of the selected security solution(s) before implementing the solution across the organization;
- Ensure that organization-issued mobile devices are fully secured before allowing user access; and
- Put in place processes to maintain and upgrade mobile device security protocols, as well as to assess the effectiveness of the organization's policies and verify that procedures are being followed.[148]

[48] In addition, in January 2015, NIST issued "Vetting the Security of Mobile Applications,"[149] "a set of standards for testing the security of

[146] *Id.* at vi–viii.

[147] *Id.* at vi.

[148] *Id.* at vi–viii.

[149] STEVE QUIROLGICO ET AL., NAT'L INST. OF STANDARDS & TECH., DEP'T OF COMMERCE, VETTING THE SECURITY OF MOBILE APPLICATIONS vi (spec. publication 800-163, Jan. 2015), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf, *archived at* http://perma.cc/6G3N-7ADS.

mobile software" that responds to concerns associated with the marked increase in the use of mobile technology that "allow[s] real-time information sharing, the ability to work from any location, and an 'unprecedented level of connectivity . . . .'"[150] In this special publication, NIST wrote that "[t]o help mitigate the risks associated with app vulnerabilities, organizations should develop security requirements that specify, for example, how data used by an app should be secured, the environment in which an app will be deployed and the acceptable level of risk for an app."[151]

[49] The proliferation of mobile apps, and security issues related to their use, is a salient concern for any organization implementing a BYOD program. NIST noted "[m]obile devices provide access to potentially millions of apps for a user to choose from. This trend challenges the traditional mechanisms of enterprise IT security software where software exists within a tightly controlled environment and is uniform throughout the organization."[152] This latest NIST publication "outlines the process for vetting a third-party application, from setting security standards to developing analytics tools to approval or rejection" of the app.[153] Although neither legally binding nor intended to take the place of any applicable standards or statutes, the NIST guidelines offer a helpful framework for reviewing key issues relevant to mobile device security in the BYOD context.

[150] Aaron Boyd, *NIST Outlines Process for Vetting Mobile Apps*, FED. TIMES (Jan. 29, 2015, 1:55 PM), http://www.federaltimes.com/story/government/mobility/2015/01/29/nist-process-securing-mobile-apps/22521427/, *archived at* http://perma.cc/LZ6B-EBP3 (quoting QUIROLGICO ET AL., *supra* note 149, at vi).

[151] QUIROLGICO ET AL., *supra* note 149, at vi.

[152] *Id.* at 2.

[153] Boyd, *supra* note 150.

B. European Union

[50] As discussed above, BYOD programs have proven less popular in Europe than in the United States, with organizations tending to follow an "allow" rather than encourage model.[154] Not only have employee preferences stifled adoption rates, but two other key considerations have slowed the progression: (1) data security concerns, with (at one time) "70 percent of organisations saying that ensuring a secure connection is the main barrier to full adoption of BYOD"[155] and (2) general European data privacy considerations, given that even deleting "*business* information and content" from a BYOD device may require employee agreement and consent.[156] Layered on top of these over-arching issues are additional country-by-country considerations, and further articulations on state, canton, and municipality levels. A brief overview of this skein—and a sense of what a real-life OEI would have to consider when doing business in Europe—follows below.

1. France

[51] In 2004, the French government adopted the most recent version of a French data protection law applicable to BYOD practices,[157] directing

[154] *See* Antony Savvas, *European Firms Allow BYOD Despite Security Concerns*, COMPUTERWORLD UK (May 23, 2012, 6:30 PM), http://www.computerworlduk.com/news/mobile-wireless/3359491/european-firms-allow-byod-despite-security-concerns/, *archived at* http://perma.cc/USK2-JV4V.

[155] *Id.*

[156] *See* Irene Bodle, *Does Your BYOD Policy Comply with Data Protection Law?*, WEB ANALYTICS WORLD (June 24, 2014), http://www.webanalyticsworld.net/2014/06/does-your-byod-policy-comply-with-data-protection-law.html, *archived at* http://perma.cc/A4SN-ZLEB (emphasis added).

[157] *See* Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties], as amended Loi 2004-801 of 6 août 2004 2004 [Law 2004-801 of August 6, 2004 relating to the Protection of Data Subjects as Regards the Processing of Personal

businesses implementing BYOD policies that involve any level of monitoring an employee's personal device to first obtain the individual's consent. Organizations implementing a BYOD policy should take reasonable security precautions to protect the data being accessed on personally owned devices. Although the law does not include a definition of "reasonable," if an organization is handling a large amount of data or particularly sensitive data, "reasonable" measures may involve precautions such as remote lock and wipe, GPS tracking, and secure web browsers and e-mail gateways.[158]

[52] Employees' expectations of privacy at work in France will depend on the context in which BYOD is being deployed. On May 23, 2012, the French Supreme Court determined an employee had an expectation of privacy on a device used at her workplace.[159] In that case, "the employee brought a personal Dictaphone to work [and] recorded conversations with her co-workers, without their knowledge or consent."[160] Her "employer discovered the Dictaphone on 'record mode'… and immediately listened to its content, while its owner was absent."[161] "The employee was consequently dismissed for gross misconduct."[162] The French Supreme

Data], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE DU 7 août 2004 [J.O] [OFFICIAL GAZETTE OF FRANCE], Aug. 7, 2004.

[158] RICHARD ABSALOM, INTERNATIONAL DATA PRIVACY LEGISLATION REVIEW: A GUIDE FOR BYOD POLICES 15 (2012), *available at* http://www.webtorials.com/main/resource/papers/mobileiron/paper5/Guide_for_BYOD_Policies.pdf, *archived at* http://perma.cc/84YK-68BL.

[159] *See* Roselyn Sands & Karlheinz Mohr, *Data Privacy Event: Bring Your Own Device*, EY 11 (2014), http://www.ey.com/publication/vwluassets/ey-bring_your_own_device/$file/ey-bring-your-own-device.pdf, *archived at* http://perma.cc/8S8P-FNRM.

[160] *Id.* at 11.

[161] *Id.*

[162] *Id.*

Court ruled that the dismissal was unjust because (1) the employer should not have listened to the recording when the employee was not present (or at least without giving the employee prior warning); and (2) the employer disregarded adversarial procedure and destroyed the recording.[163]

[53] In contrast, on February 12, 2013, the French Supreme Court found an employee did *not* have an expectation of privacy when a personal removable storage device was being used on a company-owned computer.[164] There, an employee copied her employer's and coworkers' personal and confidential files onto a personal USB key that was plugged into her company computer.[165] While the employee was out of her office, "the employer took and read the information on the USB key, and discovered the copied files."[166] As in the first case, the employee was "dismissed for gross misconduct."[167] Because "the USB key was plugged into the company's computer," the court held "the USB key was presumed to be used for professional purposes."[168] Accordingly, the employer was entitled to access files stored on the USB key that were not identified as "personal" without the employee being present or giving the employee prior warning.[169]

2. Germany

[54] In 2010, Germany's federal government approved a draft law on employee data protection which—in conjunction with other laws (such as

[163] *See id.*

[164] *See id.* at 12.

[165] *See* Sands & Mohr, *supra* note 159, at 12.

[166] *Id.*

[167] *Id.*

[168] *Id.*

[169] *See id.*

the Telecommunications Act)—applies to BYOD issues.[170] The law contains a provision addressing telecommunications services that are used exclusively for business purposes.[171] "The content of telephone calls is regulated more strictly than the content of e-mail and the Internet."[172] With respect to private use of telecommunication services in the workplace, the employer is considered to be a telecommunications services provider vis-à-vis its employees. Accordingly, the employer may not "access the content of private e[-]mail communications nor" may it access the content of "work-related e[-]mails" if separation between the two cannot be assured.[173] "Tracking and monitoring employee e-mails, even if work-related and on corporate-provisioned devices," may violate the Federal Data Protection Act "if personal e[-]mails are also allowed on the device or account."[174] Given these restrictions, implementing a BYOD program in Germany may require an organization to abandon certain types of employee monitoring.[175]

[55] In 2013, the German Federal Office for Information Security published a paper "providing an overview of the information technology risks inherent" in BYOD strategies.[176] The paper addresses a number of BYOD-related risks and "provides a list of suggested technical and

[170] *See id.* at 10.

[171] *See* ABSALOM, *supra* note 158, at 11.

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *See id.*

[176] Hunton & Williams LLP, *German Federal Office for Information Security Issues Guidance on Consumerization and BYOD*, PRIVACY & INFO. SECURITY L. BLOG (Feb. 7, 2013), http://www.huntonprivacyblog.com/2013/02/articles/german-federal-office-for-information-security-issues-guidance-on-consumerization-and-byod/, *archived at* http://perma.cc/TD44-GZDK.

organizational measures that" organizations "should implement to minimize certain risks associated with" BYOD.[177] These measures include "[s]eparating private use from professional use," "[s]ecuring connections between BYOD devices and the company network," and "[e]ntering into clear agreements with employees to establish rules regarding BYOD."[178]

[56] Also in 2013, the German Federal Office for Information Security published guidance on BYOD issues suggesting that prior to implementing a BYOD policy, organizations should verify whether the policy will comply with existing security requirements and outline the conditions to be met.[179] Devices should have "[c]urrent anti-virus programs" and "security patches," be used exclusively by the employee-owner, force "strong passwords" to prevent unauthorized access, and encrypt "[a]ll locally stored data."[180] Among other requirements, the BYOD policy should mandate immediate reporting if the device is lost; clarify which applications should not be run on the device; prohibit jail breaking the device; obtain employee consent to automated scans of the device; and specify how to deal with business data on a device when the device is "no longer used for business purposes or an employee leaves the company."[181]

[177] *Id.*

[178] *Id.*

[179] *See* Jörg Hladjk, *Germany: Guidance on Bring Your Own Device to Work — The Implementation of BYOD Strategies*, E-COMMERCE L. & POL'Y, Mar. 2013, at 5, 5, *available at* http://www.hunton.com/files/Publication/4ce88a8f-7e28-41d5-b928-9f813eb6559f/Presentation/PublicationAttachment/8218acba-2fdd-4837-b65d-02eed9d5cab2/Hladjk_Germany_guidance_on_Bring_Your_Own_Device_to_work.pdf, *archived at* http://perma.cc/8GJ3-D375.

[180] *Id.*

[181] *Id.*

3. Spain

[57] As in all EU jurisdictions, data privacy law in Spain provides individuals with rights of access, correction, erasure, and objection with respect to any of their personal data being processed.[182] "[O]rganizations planning to implement a BYOD policy should" alert employees regarding how data "will be monitored on or collected from their personal device" as employees have the right to review records their employer maintains on them.[183]

[58] In Spain, prior to 2013, the Supreme Court had directed organizations must notify employees if they were being monitored.[184] In October 2013, however, the Spanish Constitutional Court held it was permissible, even without prior notification, to monitor *company-provided* e-mail and phones, and fire an employee whose breach of confidentiality was revealed as a result of such monitoring.[185] This decision could lead more employees to push for BYOD policies to ensure that their expectation of privacy in the workplace is maintained.

4. United Kingdom

[59] In 2013, the United Kingdom's Information Commissioner's Office ("ICO") issued guidance regarding the Data Protection Act of 1998 and its application to the BYOD phenomenon, noting that BYOD raises "a number of data protection concerns due to the fact that the device is owned by the user rather than the data controller." [186] The ICO

[182] *See* ABSALOM, *supra* note 158, at 15.

[183] *Id.* at 16.

[184] *See* MELANIE LANE & KARINE AUDOUZE, INTERNATIONAL EMPLOYMENT – LATEST DIGITAL EMPLOYMENT ISSUES (2013), *available at* http://www.olswang.com/blogs/digital-employment/2013/11/2013/12/international-employment-latest-digital-employment-issues/, *archived at* http://perma.cc/GM2C-5NEF.

[185] *See id.*

emphasized that the data controller "must remain in control of the personal data for which [the controller] is responsible, regardless of the ownership of the device used to carry out [data] processing."[187] Organizations that permit staff to access data on an employee-owned device should ensure that the device is password-protected, ensure that the data is encrypted when it is transferred and stored, and consider implementing a BYOD policy for staff.[188] Notably, if data on an unsecured employee-owned device is lost, the organization and its officers—not the employee—will be held responsible.[189] Accordingly, at the very least, organizations should ensure that any "personally owned device used to access corporate data" "supports encryption."[190] Further, BYOD policies should be voluntary, and employees forced to use a personal device will expect to be compensated for the cost of purchase and use.[191] Organizations may have to supply devices to employees who choose not to agree to a BYOD policy.[192]

[60] The UK Employment Practices Code explains employees have legitimate expectations that they can "keep their personal lives private" and that they are entitled to a degree of "privacy in the work environment."[193] If organizations wish to monitor their workers by

[186] INFO. COMM'R OFFICE, BRING YOUR OWN DEVICE (BYOD) 13 [hereinafter INFO. COMM'R OFFICE], *available at* https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf, *archived at* https://perma.cc/D59A-SM6Y.

[187] *Id.* at 4.

[188] *See* Bodle, *supra* note 156.

[189] *See* ABSALOM, *supra* note 158, at 12.

[190] *Id.* at 13.

[191] *See id.*

[192] *See id.*

collecting information on them—for example, "[recording] video [of] workers to detect crime," check[ing] telephone logs to detect excessive private use," or monitoring e-mails and Internet use—"the Data Protection Act will apply."[194] Although the Data Protection Act allows monitoring, it instructs organizations to be clear about the purpose of the monitoring and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered.[195]

[61] The UK ICO released a quick guide on the employment practices code that instructs small businesses on how the Data Protection Act affects monitoring and what businesses can do if they want to monitor workers.[196] Organizations must ensure their employees "are aware that they are being monitored and why" the monitoring is occurring.[197] Because employees are entitled to some privacy in the workplace, organizations should be particularly careful when "monitoring communications, such as e-mails, that are clearly personal."[198] For example, they should monitor the message's address and heading only, and "[a]void wherever possible opening e-mails, especially those that clearly [suggest] they are [of a] private or personal" nature.[199] Further, if it is necessary to check the e-mail accounts or voicemails of employees in their absence, organizations must ensure employees are aware this will happen.[200]

---

[193] INFO. COMM'R OFFICE, QUICK GUIDE TO THE EMPLOYMENT PRACTICES CODE 14 (2011), *available at* https://ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf, *archived at* https://perma.cc/G93M-DW77.

[194] *Id.* at 13.

[195] *See id.* at 13–14.

[196] *See id.* at 13–16.

[197] *Id.* at 15.

[198] *Id.* at 16.

[199] INFO. COMM'R OFFICE, *supra* note 186, at 16.

[62] A recent U.S. federal court case involving the UK may have interesting implications for monitoring in the BYOD context. In *United States v. Odoni*, the U.S. Court of Appeals for the Eleventh Circuit held "[t]he Fourth Amendment's private search doctrine applies even when the 'private' search is conducted by foreign law enforcement authorities."[201] In *Odoni*, the defendant Paul Robert Gunter was a British national and permanent U.S. resident who was found guilty of participating in two investment fraud schemes.[202] "The defendant's laptop and thumb drive were taken from him by U.K. investigators when he was arrested while stepping off a plane at an airport in the U.K."[203]

[63] Gunter "did not allege that the federal agents asked the foreign investigators to conduct a search of [his] laptop and thumb drive. Instead, the defendant contended that the foreign investigators had only seized the devices and not searched the data."[204] After the British investigators conducted the initial search, they sent copies of the laptop's hard drive and the thumb drive to agents with the U.S. Secret Service and U.S. Department of Homeland Security.[205] The U.S. "federal agents searched the data sent by the U.K. agents and used it [to] obtain warrants to search

---

[200] *See id.*

[201] Hugh Kaplan, *Search and Seizure: Foreign Investigators' Warrantless Search Permits Warrantless Search by U.S. Agents*, BLOOMBERG BNA EDISCOVERY RESOURCE CENTER (Jan. 14, 2015), http://ediscovery.bna.com/edrc/7082/split_display.adp?fedfid=61889988&vname=ddeenotallissues&jd=a0g1q3w9m0&split=0, *archived at* http://perma.cc/EH42-P8JJ (citing United States v. Odoni, No. 13-13528, 2015 U.S. App. LEXIS 502, at *31 (11th Cir. Jan. 13, 2015)).

[202] Kaplan, *supra* note 201 (discussing *Odoni*, 2015 U.S. App. LEXIS 502, at *14).

[203] *Id.* (discussing *Odoni*, 2015 U.S. App. LEXIS 502, at *19–20).

[204] *Id.*

[205] *See Odoni*, 2015 U.S. App. LEXIS 502, at *21–22.

the defendant's business premises and online Quick Books account."[206] The Eleventh Circuit held that, since an entity other than a U.S. state or federal official had already examined the contents of the devices, Gunter no longer had a reasonable expectation of privacy in their contents.[207] Judge Susan H. Black reasoned:

> Although the third party who conducted the prior search in *Jacobsen* [where the court determined that an individual does not have a reasonable expectation of privacy in an object to the extent the object has been searched by a private party] was a private actor, the reasoning in *Jacobsen* applies with equal force when the third party who conducts the prior search is a foreign governmental official.[208]

V. CONCLUSION: CONSIDERATIONS FOR IMPLEMENTING OR IMPROVING A BYOD PROGRAM

[64] As demonstrated by our review of the various legal considerations and practical implications concerning the implementation of cross-border BYOD programs, this is not an area that lends itself to straightforward answers. At present, there are no specific "Do's and Don'ts" that would apply uniformly in all cases, so an organization-oriented approach is essential. Stakeholders within the organization—including the IT Department, the Legal Department, Human Resources, and others as appropriate—should thoroughly discuss proposed policies and procedures to assess how to construct a BYOD program that serves the organization's business needs while complying with applicable laws and regulations. To facilitate the process of designing and implementing (or improving) a BYOD program, below we provide a list of considerations for review and discussion. As rapidly-evolving BYOD technology continues to challenge

[206] Kaplan, *supra* note 201 (discussing *Odoni*, 2015 U.S. App. LEXIS 502, at *21–22).

[207] *See Odoni*, 2015 U.S. App. LEXIS 502, at *31.

[208] *Odoni*, 2015 U.S. App. LEXIS 502, at *27.

a shifting legal landscape, organizations with BYOD concerns should pay close attention to developments in this area and adjust their strategies accordingly.

A. Considerations Pertaining to the Device Itself

- What types of devices will the organization support?[209]
    - If a wide variety of devices will be supported, how will the organization provide a consistent employee-user experience?
- Should Mobile Device Management Solutions ("MDMs") be implemented?[210]
- Would the organization be better served by a "corporate-owned, personally enabled ("COPE")" or a "corporate-owned, business-only ("COBO") strategy?[211]
- Are certain devices—or their operating systems—subject to export controls?
- If employees will be reimbursed for device purchases, how will the reimbursement process work?
- How will the organization address device disposal/employee separation issues?
- What happens when a device is lost or stolen?
    - If an employee wishes to trade in a device containing company data, how will the organization ensure that all such data is securely removed from the device?
    - How can the organization ensure data security with respect

[209] *See* Bodle, *supra* note 156.

[210] *See* Woodworth, *supra* note 1, at 4; *see also* GARY G. MATHIASON ET AL., THE "BRING YOUR OWN DEVICE" TO WORK MOVEMENT: ENGINEERING PRACTICAL EMPLOYMENT AND LABOR LAW COMPLIANCE SOLUTIONS 50–51 (2012), *available at* http://www.littler.com/files/press/pdf/TheLittlerReport-TheBringYourOwnDeviceToWorkMovement.pdf, *archived at* http://perma.cc/M32S-PAMS.

[211] HETTING, *supra* note 8, at 2.

to company data on a personal device if an employee is terminated or otherwise separates on bad terms?
- How will the organization recover company data if an employee inadvertently (or intentionally) deletes it from a BYOD device?

B. Considerations Regarding Device Usage

- Who within the organization will be allowed to participate in the BYOD program[212] and will the scope of employee participation differ depending on job functions?[213]
- What types of company data may employees access using their devices?[214]
- Will the organization pay (or reimburse) data plan charges? What about overages, roaming charges, or other associated expenses?[215]
- What are the organization's overtime and other wage-and-hour considerations with respect to BYOD use outside of normal working hours?[216]
- Who owns the data on the device when an employee leaves?[217]
- How should the organization restrict "risky" employee behavior on the clock (for example, by implementing "policies . . . that prohibit or reduce the risk of workers texting or otherwise using their devices while driving?")[218]

[212] *See* Bodle, *supra* note 156; *see also* MATHIASON ET AL., *supra* note 210, at 45.

[213] *See* McLaughlin, *supra* note 84; *see also* MATHIASON ET AL., *supra* note 210, at 45–46.

[214] *See* Bodle, *supra* note 156; *see also* MATHIASON ET AL., *supra* note 210, at 51.

[215] *See* Cochran v. Schwan's Home Serv., Inc., 228 Cal. App. 4th 1137, 1140 (2014); *see also* McLaughlin, *supra* note 84.

[216] *See* MATHIASON ET AL., *supra* note 210, at 46.

[217] *See* Bodle, *supra* note 156.

- Will the organization need to restrict the use of BYOD for certain types of *work* activity (for example, when legal holds create preservation and collection burdens)?

C. Policy Development Strategy

- What considerations go into the organization's strategic approach?
    - For compliance and liability purposes, the organization must dictate policy, but is an organization-wide policy appropriate when operations vary widely within the organization?
    - A traditional top-down approach, with the organization giving specific instructions to employees, may offer certain benefits.
        - At least one commentator has hypothesized that, "[c]ustomers are more likely to choose suppliers who demonstrate that they control and monitor the use of business and customer data on BYODs. Having a clear BYOD policy in place will often satisfy a customer's security concerns about the use and storage of personal data on mobile devices."[219]
        - Even if the employee does not follow directions perfectly (or at all), a consistently-enforced, well-structured BYOD policy may help shield the organization from potential liability.
    - Some organizations set policy on the business-unit level to allow for business purpose and related flexibility. This type of bottom-up approach, empowering employees to make their own decisions guided by principles implemented at a higher level, theoretically benefits productivity, but also increases complexity and may increase risk.

[218] Hetting, *supra* note 8, at 13.

[219] Bodle, *supra* note 156.

- How will the organization handle BYOD policy violations?[220]
- How will the organization address border crossing security issues with respect to BYOD devices? Relevant policies must consider potentially hostile countries with traditionally strict data control measures (e.g., China and the great firewall) as well as the possibility of employee devices being searched at the U.S. border by U.S. authorities.[221]
- Will the organization attempt to employ a "business use only" policy as discussed in the NLRB's *Purple Communications* decision?[222]
    - Employers may face potential liability for any "business use only" policies in instances where "employees who have already been granted access to the employer's e-mail system in the course of their work" must also be allowed to use that e-mail system to communicate with colleagues about workplace concerns, even during non-working hours.[223]
    - Organizations with existing or planned "business use only" policies regarding employee use of company e-mail may need to revisit and revise them.
- What device security considerations are involved at the strategic level? These considerations may include the following:
    - Policy guidelines requiring a certain type of password;
    - The installation of monitoring/wiping software; or
    - Requiring acknowledgement of organizational guidelines on a regular basis (e.g., through a pop-up).
- Which jurisdiction's law will apply in various scenarios?

[220] *See id.*

[221] *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 956 (9th Cir. 2013) (en banc); United States v. Arnold, 533 F.3d 1003, 1005 (9th Cir. 2008).

[222] *See* Purple Commc'ns, 361 N.L.R.B. No. 126, 2014 NLRB LEXIS 952, at *8–10 (Dec. 11, 2014).

[223] *Id.* at *4.

  - Is the location of the organization's headquarters the primary determinant?
  - How relevant is each individual employee's location? What if an employee works out of multiple offices or travels frequently?
  - How will the organization apply multiple jurisdictions' laws or regulations consistently?
    - Consistency is perhaps the best defense when the law is uncertain. Organizations following this approach should aim to develop policies that hew as closely as possible to the ostensibly applicable laws and then enforce those policies across the board.
    - As a rule, it is preferable to avoid implementing policies if the organization knows that violations are inevitable.
- How will the organization integrate BYOD considerations into other organizational policies? Such policies may include:
  - "Harassment, Discrimination, and Equal Employment Opportunities;
  - Workplace Safety;
  - Time Recording and Overtime;
  - Acceptable Use of Technology;
  - Compliance and Ethics;
  - Records Management;
  - Litigation Holds; [and]
  - Confidentiality and Trade Secret Protection."[224]

D. Privacy Concerns and Other Legal Considerations

- Who within the organization is responsible for monitoring legal developments concerning BYOD?
  - How will the organization consider and apply forthcoming revisions to the EU Data Protection Regulation?
  - Should the organization obtain local counsel advice before

[224] MATHIASON ET AL., *supra* note 210, at 45.

proceeding with a BYOD program in foreign jurisdictions?

- How will the organization provide notice of its monitoring practices, and offer choices with respect to monitoring where required?
    - In the U.S., organizations may expose themselves to liability for unfair or deceptive trade practices if they go beyond what they say they will be doing in terms of monitoring, or if they exploit their access to employee device information beyond what is necessary for legitimate business interests.
    - Notice and choice with regard to monitoring practices may be legally required in certain jurisdictions.
    - In the EU, it may be impossible to obtain valid consent in the employment context, as the employee/employer relationship may be viewed as necessarily coercive in nature.
- What additional factors should be considered when the organization issues legal holds that apply to BYOD devices?
    - Who should draft the policy?
    - How should the organization apply the policy and publicize it to employees?