THE LITTLER REPORT

THE "BRING YOUR OWN DEVICE" TO WORK MOVEMENT:

Engineering Practical Employment and Labor Law Compliance Solutions

May 2012

AUTHORS

Garry G. Mathiason
Michael J. McGuire

Gavin S. Appleby
Philip M. Berkowitz
Tanja L. Darrow
Helena Eldemir
Philip L. Gordon
Jacqueline A. Gruber
Ben Huggett
Earl M. (Chip) Jones, III
Stacey E. James
Sara B. Kalis
Henry D. Lederman
Chris M. Leh
Johan Lubbe
Cecil A. Lynn
Suellen Oswald
Todd M. Ratshin
George M. Reardon
Mark W. Schneider
Paul D. Weiner
William Hays Weissman
Dylan W. Wiseman
Jennifer A. Youpa

Littler
Employment & Labor Law Solutions Worldwide™

IMPORTANT NOTICE

This publication is not a do-it-yourself guide to resolving employment disputes or handling employment litigation. Nonetheless, employers involved in ongoing disputes and litigation will find the information extremely useful in understanding the issues raised and their legal context. The Littler Report is not a substitute for experienced legal counsel and does not provide legal advice or attempt to address the numerous factual issues that inevitably arise in any employment-related dispute.

Table of Contents

SECTION / TOPIC	PAGE
I. **INTRODUCTION**	1
II. **BACKGROUND**	3
A. The Consumerization of Information Technology	3
B. Adoption of BYOD Policies	4
C. A Cost/Benefit Decision for Employers	6
D. The "Appification" of Corporate Information Technology	7
E. Challenges for Employers	8
III. **DATA-RELATED CHALLENGES OF BYOD PROGRAMS**	10
A. Information Security Risks for the Employer's Information	10
B. Record Management Laws and Contractual Obligations	13
C. The Privacy of Employee Data on Dual-Use Devices	13
D. Preserving and Collecting Data from Employees' Dual-Use Devices for Litigation Holds and Investigations	16
E. Protection of Trade Secret Information on Dual-Use Devices	24
F. Use of Dual-Use Devices By Contingent Workers	28
IV. **BEHAVIOR-RELATED CHALLENGES OF BYOD**	30
A. Performance Management	30
B. Equal Employment Opportunity & Dual-Use Devices	30
C. Wage & Hour Issues	35
D. Workplace Safety and Health (OSHA)	39
E. Deploying BYOD in a Unionized Workforce	41
F. International Legal Challenges	43
V. **RECOMMENDATIONS**	45
A. Implement New Policies	45
B. Develop Employee Agreements	49
C. Implement Technical Controls	50
D. Implement New or Revised Operating Procedures	52
E. Training	54
F. Risk Management Approach	54
VI. **CONCLUSION**	56
ENDNOTES	57
APPENDIX A: CHECKLISTS FOR DEVELOPING A BYOD PROGRAM	58

THE "BRING YOUR OWN DEVICE" TO WORK MOVEMENT:

Engineering Practical Employment and Labor Law Compliance Solutions

I. INTRODUCTION

Two different, but interrelated, phenomena have been occurring over the last decade that are radically reshaping the work environment at many companies. The first is commonly referred to as the "Consumerization of Information Technology." The second is the blurring of the line between work life and personal life experienced by many employees.

One result is the rapid adoption of mobile devices by employees–including iPhones, iPads, Android smartphones, and other devices. Due to their ease of use and the functionality enhanced by hundreds of thousands of free or low-cost applications available for these devices, millions of employees have begun using them to perform work. Recognizing this, a growing number of companies have struggled to create new policies that allow employees to use their personal mobile devices to create, store, and transmit work-related data. These new policies turn an employee's personal device into a "dual-use" device, one used for both personal and company data and activities. This trend is generally referred to as "Bring Your Own Device" or BYOD. Some companies even allow their employees to replace their work laptop computer with their own personal PC, which is sometimes referred to as BYOC.

This Littler Report examines the development of this irreversible trend and explores the very real and immediate challenges–both practical and legal–it creates for employers. Thereafter we set forth a series of recommendations to assist employers in mitigating these risks as the BYOD movement continues to reshape the workplace and even the concept of "a" workplace.

The risks fall into two broad categories. The first set of risks relates to the fact that a company's data is now being stored and transmitted using devices and networks the employer may not own or control. This loss of control clashes with the growth over the last decade of government regulations requiring companies to carefully protect the privacy and security of sensitive personal, financial, and health-related data. It also poses risks to the protection of a company's trade secret, proprietary, or confidential information.

The second set of risks arises from the impact BYOD policies may have on the behavior of employees. For example, employees may feel the use of their own personal devices should not be regulated by company policies on acceptable use, or they may be more likely to engage in "off-the-clock" work that could either increase overtime expenses or the risk of wage and hour claims. Employees may be more inclined to access in the workplace immediately available images and other material that could be in conflict with harassment prevention policies. This is different from the past decade where employers could set limits on usage because they owned and had more control over workplace computers and mobile devices.

Many of these risks can be addressed through the use of new types of software, typically referred to as Mobile Device Management software, that give employers a measure of control over their employees' dual-use devices. But this software can only mitigate, not eliminate, these risks. Employers must also consider revising or creating new policies and operating procedures, entering into new or supplemented employee agreements, and developing a broad awareness of these issues among their employees. This is more than rewriting the company's Acceptable Use Policy. The BYOD movement requires consistency across multiple workplace policies and practices.

Several of the risk areas discussed in this Report also apply to company-owned mobile devices, but the focus of this Report is on identifying challenges for companies that are pursuing BYOD policies or are reacting to the inevitable use of personal devices in the workplace.

We focus this Report on the BYOD movement because the light-speed growth of consumer technology, and the lifestyle plus skills of new generations, increasingly are clashing with traditional ways of mitigating employment and labor law risk. A new set of solutions is desperately needed. Many employers have already built pathways for the BYOD Movement. Littler predicts that within no more than one to three years virtually every employer will have confronted this issue and a majority will have harnessed the positive energy and advantages of the Movement while mitigating risk through new technology, revised policies and practices, and employee education.

II. BACKGROUND

A. The Consumerization of Information Technology

The phrase the "Consumerization of IT" was coined in 2001 by researchers at Computer Sciences Corporation (CSC). They used the phrase to describe "the radical reorientation of the IT industry" they saw taking shape in many companies because of the emergence of consumer technologies.[1] In 2004, the same CSC researchers published a Position Paper, *The "Consumerization" of Information Technology*.[2] The Paper described their observations and findings about how consumer-based technologies, public (as opposed to private) infrastructure, and applications had the potential to dramatically lower the cost and improve the functionality of corporate IT departments. Several of their key findings are highly relevant to the BYOD discussion; some are even prescient. For that reason, their findings are restated in their entirety below.

- Consumerized technologies, infrastructure and applications can deliver ***dramatically lower costs and equally significant improvements in business functionality and ease of use***. While most of these technologies have been on the radar screen for several years, we believe that they are now reaching critical mass, and that organizations need a process for adjusting to these developments.
- Enterprises have usually supported IT with private infrastructures. There is growing tension between this traditional sourcing model and the consumerized alternatives that are now available. Over time, ***comprehensive private IT infrastructures will become a luxury*** that even the biggest organizations cannot afford. We believe that consumerization will be the process by which many of these traditional infrastructures are transformed and revitalized.
- In many organizations, ***existing infrastructures and their supporting policies and assumptions have become a barrier to innovation*** and a source of increasing employee frustration with corporate IT. The potential conflicts between exciting new consumerized services and ageing business infrastructures must be minimized. CIOs must be on the side of change.
- Consumerization seems likely to be a classic case of "disruptive" technology, which means many organizations will find it difficult to manage. To exploit consumerized technology and public infrastructure successfully, ***companies must decide to support this transition and then learn to scan, evaluate and judge service maturity***.
- CIOs will eventually be asked to integrate these new services with existing business systems. This will prove a daunting challenge, and will show that ***some consumer services are not as cheap as they first appear***.
- Although the ***security issues are often very real*** and can in the short term be only partially addressed, they should not be allowed to stop emerging consumer infrastructure usage. Over time, market pressures will push many consumer systems to match or exceed the security of privately managed systems. In some areas, this has already happened.

1 David Moschella, *What the Consumerization of IT means to your business, ten messages for CXOs*, *at* http://lef.csc.com/blog/post/2011/06/what-the-consumerization-of-it-means-to-your-business-ten-messages-for-cxos.

2 David Moschella, Dou Neal, and John Taylor, *The 'Consumerization' of Information Technology*, Computer Sciences Corp, 2004.

- ***Companies must treat users as consumers***, encouraging employee responsibility, ownership and trust by providing choice, simplicity and service. ***The parent/child attitude*** that many IT departments have traditionally taken toward end users ***is now obsolete***.
- To take advantage of consumerization, ***companies must acknowledge and leverage the blurring of our personal and professional lives***. This means adopting differentiated employee usage and support models. The traditional top-down, one-size-fits-all approach will increasingly alienate employees and result in lost business opportunities.
- As the current pace of technology improvement is expected to continue for many years, these issues are sure to become more important. Companies that gain an early understanding of consumerized technologies and their related issues will have significant cost and usage advantages.

(Emphasis added.)

Over the last few years–primarily due to the broad popular appeal of the iPhone, the iPad, and Android devices–the consumerization trend has accelerated. In fact, in April of 2012, Apple created a new feature on its website called iPhone at Work. The page lists apps designed to help you organize your day, view your business, manage projects, meet anywhere, and travel light. The broad appeal of these devices, coupled with their rapid adoption by consumers, has caused many CIOs to begin allowing these devices to interact with corporate IT systems and even replace company-owned devices.

According to one recent study that aggregated data from multiple sources, there is a shift away from laptops and PCs towards smartphones and tablets. In 2010, 350.8 million personal computers were sold worldwide. During the same timeframe, 296.6 million smartphones and 17.6 million tablets were sold. For 2011, the estimates were that 364 million PCs would be sold, but 468 million smartphones and 63.6 million tablets would be sold. The trend will continue with tablet sales predicted to roughly equal overall PC sales by 2015.[3]

B. Adoption of BYOD Policies

According to a global study by the Aberdeen group in July 2011, of 415 companies surveyed, 75 percent allowed employees to use their personal mobile devices for business purposes.[4] Another survey by Forester Research showed similar adoption rates of BYOD. In their study from the Fall of 2011 of roughly 1,600 US information technology workers, Forester found that 48 percent of those responding were able to purchase the smartphone of their choice and use it for work.[5] A 2011 study by IDC and Unisys of 3,000 information workers and business executives in nine countries showed that more than 40% of the devices used by respondents to access business applications were personal devices. This is a 10% increase from a 2010 study. The study also shows that work is intruding on personal life. Approximately 50% of respondents reported using personal devices to conduct work on vacation, 29% while in bed, and almost 20% while

3 David Meyer, *Sales of Smartphones and Tablets to Exceed PCs*, Oct. 6, 2011, Practical eCommerce, Insights for Online Merchants, *available at* http://www.practicalecommerce.com/articles/3069-Sales-of-Smartphones-and-Tablets-to-Exceed-PCs-.

4 Dave Zielinski, *Bring Your Own Devices*, Society for Human Resource Management, Vol. 51, No. 2, *available at* http://www.shrm.org/Publications/hrmagazine/EditorialContent/2012/0212/Pages/0212tech.aspx.

5 *Id.*

driving. A surprising 5% reported using the devices in a place of worship. They also use their devices to perform work during "down time" (vacations and watching TV) and while at family gatherings.[6]

Perhaps the largest company to adopt a BYOD policy is IBM, which recently started a BYOD program. At present, only 80,000 IBM employees use their own personal devices, but the company hopes to extend the program to include all 440,000 employees.[7] Although IBM had traditionally offered corporate-owned and managed Blackberries, iPhones and other devices started making an appearance. IBM's CIO decided that "If we didn't support them, we figured [employees] would figure out how to support [the devices] themselves."[8] This self-directed approach would have been a problem for IBM given the volumes of sensitive information that could have been put at risk. According to IBM's CIO, employees "will find the most appropriate tool to get their job done. I want to make sure I can enable them to do that, but in a way that safeguards the integrity of our business."[9]

As one way of mitigating the risks to company data, IBM is building what they call "fit for business" tools that offer the functionality of popular consumer-level tools, but which include the security features IBM requires. One example is an IBM version of the popular cloud-based remote storage service Dropbox.[10]

As another example, Kraft Foods started a BYOD program in 2010. Kraft gives approximately 800 employees a stipend to buy either a Windows or Mac computer. If an employee wants a computer that costs more than the stipend amount, the employee must pay the difference. The Kraft program is not available to company executives who handle confidential information, Legal or HR staff, or employees who use their PC to run production equipment. Factory workers are also not eligible.[11]

Sybase, a 4,000-employee company, has developed a policy that embraces BYOD. Sybase makes and sells software (called Afaria) that allows employers to control dual-use devices. Sybase has leveraged this software for its own internal operations.[12] Under the Sybase approach:

- Employees can choose from 20 different phones.
- Employees buy and own the phones, but Sybase pays for the monthly service contract.[13]
- Sybase apps such as Mobile Office for work email and contacts can be installed and run on those phones.

Employees must let Sybase use its Afaria software to wipe their devices and delete company data if they are lost or stolen, or if the employees leave the company.[14]

---

6 Frank Gens, Danielle Levitas, and Rebecca Segal, *2011 Consumerization of IT Study: Closing the "Consumerization Gap"*, July 2011.

7 Chris Kanaracus, *IBM CIO discusses Big Blue's BYOD strategy*, COMPUTERWORLD, Mar. 26, 2012, http://www.computerworld.com/s/article/9225563/IBM_CIO_discusses_Big_Blue_39_s_BYOD_strategy.

8 *Id.*

9 *Id.*

10 *Id.*

11 Verne G. Kopytoff, *More Offices Let Workers Choose Their Own Devices,* Sept. 22, 2011, http://www.nytimes.com/2011/09/23/technology/workers-own-cellphones-and-ipads-find-a-role-at-the-office.html?pagewanted=all.

12 JP Finnell, *Transient Apps: The Consumer Influence on Enterprise Mobility, Part 2*, GigaOm, Aug. 2010.

13 Dave Zielinski, *Bring Your Own Devices*, Society for Human Resource Management, Vol. 51, No. 2, *available at* http://www.shrm.org/Publications/hrmagazine/EditorialContent/2012/0212/Pages/0212tech.aspx.

14 *Id.*

Citrix, a company that sells software to virtualize the corporate desktop and make it available remotely to workers, adopted a BYOD program in 2008. Citrix gives each employee a $2,100 stipend to purchase a laptop of their choice and a 3-year warranty. Citrix's internal cost for similar equipment and service was $2,600. Citrix reports an adoption rate of about 20%. By using their own desktop virtualization software, Citrix ensures that sensitive corporate data stays on secure corporate servers and is not stored on employee devices, thus mitigating many of the data-related risks described in this Littler Report.[15]

C. A Cost/Benefit Decision for Employers

Many companies that are adopting dual-use device policies are doing so because they believe this approach has significant benefits for both the company and their employees, including:

- Reducing expenses for employers (estimated to be approx. $80 per employee per month for device, cellular access, etc.) by allowing companies to leverage their employees' investments in devices
- Improving employee engagement because employees can use devices they want and already know how to use
- Aiding in the recruitment of new employees
- Solving the "two pocket problem" by allowing employees to carry only one device, rather than two–one for business and one for personal use
- Allowing companies to more quickly take advantage of newer technologies that reduce cost and promote collaboration

This "common sense" approach that is gaining acceptance is not without challenges and concerns. Some recent research suggests that BYOD programs have hidden costs that may cause companies to spend more money than they realize and could make the programs more expensive to operate than the traditional model. A recent article in CIO magazine[16] describes these hidden costs.

First, employers lose the power of bulk purchasing and the ability to demand discounts from device manufacturers and cellular providers when their employees purchase individually. These higher costs hit the company through employee expense reimbursements, with a cost differential as much as $10 a month per device per employee.

Second, some companies experience higher help desk and support costs because employees use multiple platforms on many different devices, making it harder and more expensive to support them. And, employers who decide to create their own internal mobile device applications (or "Apps") are faced with the prospect of developing them for multiple platforms as opposed to a single corporate standard.

Security is also another expensive item for employers. In a recent survey by Aberdeen of more than 600 IT decision makers, they discovered that more than half of the companies reported experiencing a security breach as a result of consumer gadgets.

15 *Id.* http://www.shrm.org/Publications/hrmagazine/EditorialContent/2012/0212/Pages/0212tech.aspxhttp://www.shrm.org/Publications/hrmagazine/EditorialContent/2012/0212/Pages/0212tech.aspx.

16 *See* Tom Kaneshige, *"BYOD" If You Think You're Saving Money, Think Again*, CIO Magazine, Apr. 4, 2012, *available at* http://www.cio.com/article/703511/BYOD_If_You_Think_You_re_Saving_Money_Think_Again.

The article concluded with this sobering fact:

> All tallied, BYOD doesn't look pretty from a cost perspective. A typical mobile ***BYOD environment costs 33 percent more*** than a well-managed wireless deployment where the company owns the devices ***."

(Emphasis added.) If the perceived cost savings are the primary driver for a company–as opposed to the cultural, flexibility, or employee engagement benefits–companies should evaluate the cost savings closely before making this fundamental change. The total cost debate is far from settled and will change over time.

D. The "Appification" of Corporate Information Technology

The consumerization trend goes beyond merely the devices employees use to access, store, and transmit data. It also extends to the applications and services they use with the devices to conduct business. Given the low-cost, or even free, applications that are available to mobile device users via the Apple Store or the Android Marketplace, it is not surprising that employees are beginning to adopt these consumer-level applications and leverage them for business. After all,

> "[w]hat are employees supposed to think when the e-mail systems they get for free at home seem so much simpler, more reliable and more functional than the expensive ones they are forced to use at work? How is it possible to the average consumer can set up a wireless LAN at home in a few hours, while corporate IT takes months, or deems the whole idea too difficult?"[17]

In addition, some predict the growth of transient apps, which are described as a new category of enterprise App that meets the needs of multi-tasking workers who can use an App to meet a specific purpose and then dispose of it. Such apps are generally simple apps that are "lightweight, custom, easy to integrate, not mission-critical (relative to mobile enabled ERP or CRM business apps), self-service, low-cost, take less than two weeks to develop and often 'mash up' data from internal and external sources." Examples of such transient apps include things such as corporate conference apps, resource scheduling apps, project management apps, brainstorming apps, and time and expense reporting apps.[18] These "quick and dirty" apps will supplement more traditional applications as well as new mobile apps that allow easier access to traditional corporate IT systems, including Customer Relationship Management software or other enterprise applications.[19]

Some companies are embracing this "Enterprise App" trend and have started developing applications specifically for their employees to help them accomplish their jobs. For example, Genentech has built an enterprise App store stocked with third-party applications that employees can use to get their job done. This has created a new mentality of "*I have an app for that.*"[20] Other vendors offer software to allow mobile employees to access corporate SharePoint sites securely.

17 David Moschella, Dou Neal, and John Taylor, *The 'Consumerization' of Information Technology, supra* n. 2 at 4.

18 JP Finnell, *Transient Apps: The Consumer Influence on Enterprise Mobility, Part 2,* GigaOm, Aug. 2010.

19 *Id.*

20 *Id.*

Companies are also developing marketplaces for apps targeting specific industries, such as Happtique, a mobile App store for hospitals and healthcare professionals. It offers a catalog of mobile health apps that are designed to connect patients to their healthcare providers and physicians through mobile phones. The platform is being used by hospitals such as Mount Sinai Hospital and Beth Israel Medical Center.[21]

E. Challenges for Employers

The move to greater adoption of mobile devices is clearly accelerating and appears irreversible. They provide workers with too much flexibility and convenience to be ignored. The question for employers is how to respond to this trend. There are several options, including providing employees with a wider variety of corporate-owned mobile devices to allow employees to use the device of their choice and loosening restrictions on use of these devices for personal activity. Another option, which is currently enjoying a surge in popularity, is to allow employees to use their personally owned devices to perform work and adopt BYOD programs. The remainder of this Report describes the challenges a BYOD approach creates for employers and provides practical recommendations employers can consider to mitigate the risks.

These developments pose two types of challenges for organizations. First, companies that adopt a BYOD policy now have their corporate data stored on personal devices owned by their employees. This creates several data-related challenges for companies, especially those in highly regulated environments, such as healthcare, financial services, and those that handle sensitive personal information. Second, because employees are using devices they own, it may change their expectations regarding what constitutes appropriate use of the device. This change could create significant conflict with other company policies.

In fact, recent research shows the personal "ethics" or "morals" of some workers who are active "social networkers" sharply diverge from other workers on key issues. In the 2011 National Business Ethics Survey (NBES), the Ethics Resource Center reported that active social networkers (defined as an employee who spends 30% or more of his or her work day participating on various social network sites) are more likely to believe that certain questionable behaviors are acceptable. The table below shows the responses to several questions by those who are active social networkers compared with other US workers.

21 Rip Empson, *Happtique Brings Secure, Branded App Stores To Hospitals And Healthcare*, Dec. 7, 2001, *at* http://techcrunch.com/2011/12/07/happtique-brings-secure-branded-app-stores-to-hospitals-and-healthcare/.

Do you feel it is acceptable to...?	Active Social Networkers	Other U.S. Workers
"Friend" a client/customer on a social network	59%	28%
Blog or tweet negatively about your company or colleagues	42%	6%
Buy personal items with your company credit card as long as you pay it back	42%	8%
Do a little less work to compensate for cuts in pay or benefits	51%	10%
Keep a copy of confidential work documents in case you need them in your next job	50%	15%
Take a copy of work software home and use it on your personal computer	46%	7%
Upload vacation pictures to the company network or server so you can share them with co-workers	50%	17%
Use social networking to find out what my company's competitors are doing.	54%	30%

While these findings may not be generally applicable to all mobile workers, these potential changes in expectations and attitudes, combined with the dispersion of corporate data to devices beyond the corporation's immediate control, deserve considerable attention. Companies should consider these issues when crafting policies and procedures to accompany the rollout of a BYOD program.

III. DATA-RELATED CHALLENGES OF BYOD PROGRAMS

The move to dual-use devices raises several challenges because company data is no longer stored on devices the company owns and can control. These challenges arise in the area of security and privacy, litigation holds, record retention obligations, trade secret protection, and more.

A. Information Security Risks for the Employer's Information

Dual-use devices can expose businesses' sensitive information to unauthorized acquisition in many ways. In a recent survey of 614 senior-level IT security professionals, 76% of the respondents reported that employees' use of mobile data-bearing computing devices, such as smartphones and tablets, created a "significant" or "very significant" risk for their organizations' security posture.[22]

1. Lost or stolen devices

The most obvious risk is the loss or theft of a dual-use device. According to a study of security breaches published by the Ponemon Institute in 2011, a leading information security think tank, lost and stolen equipment was the number one cause of surveyed security breaches, accounting for 31% of surveyed breaches.[23] In a more recent study by Ponemon, 39% of respondents reported that their organizations had sustained a data security breach in 2011 as a result of lost or stolen equipment.[24] In 2011, Lookout, a company that provides software to help locate lost or stolen devices, helped 9 million people locate their devices. That corresponds to one locate request every 3.5 seconds.

2. Malware

Even if a dual-use device is not lost or stolen, the device can create security risks in other ways. For example, in February 2012, Juniper Networks reported a 155% increase from 2010 to 2011 in the volume of malicious software created for mobile devices.[25] Some of this malicious software takes the form of apparently innocuous applications ("Apps") downloaded to the dual-use device, particularly devices running the Android operating systems. While Apple screens Apps offered through its App Store, the Android Market does not, and anyone can submit an App for downloading. As a result, applications available for that platform are more likely to be malicious. In fact, in the last seven months of 2011 alone, Juniper found "***malware targeting the Android platform rose 3,325 percent***."[26] The sophistication of the attacks is also increasing. One reflection of this potential exploit is the Ponemon Institute's finding that insecure mobile devices were the fourth most common cause of the loss or theft of corporate data, accounting for 13% of the surveyed breaches.[27]

22 Ponemon Institute, *Future State of IT Security: A Survey of IT Security Executives*, Feb. 2012, *available at* http://365.rsaconference.com/servlet/JiveServlet/download/17366-3683/RSAC+Manuscript+FINAL+7.pdf, at 6.

23 Ponemon Institute, *Understanding Security Complexity in 21st Century IT Environments*, Feb. 2011, *available at* http://www.checkpoint.com/downloads/whitepapers/ponemon-check-point-march2011.pdf, at 10.

24 Ponemon Institute, *2011 Cost of Data Breach Study: United States*, Mar. 2012, *available at* http://bit.ly/xBF6vr, at 10 (shortened URL link directs to report on Symantec website).

25 Juniper Networks, 2011 Mobile Threats Report, Feb. 2012, at 6, *available at* http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf?utm_source=promo&utm_medium=right_promo&utm_campaign=mobile_threat_report_0212.

26 *Id.* at 8.

27 Ponemon Institute, *Understanding Security Complexity in 21st Century IT Environments, supra* note 22, at 10.

3. Friends and family

While hackers are commonly believed to be the greatest threat to sensitive information, the reality is that friends, family members and housemates can pose an even more significant risk to sensitive information stored on a dual-use device. When an employee shares a dual-use device with others perceived as trustworthy, or leaves the device unattended in an apparently friendly environment, a trusted person likely would have no need to bypass security measures, such as encryption or password protection because the device would already be unlocked. To be sure, the idea that an employee's "circle of trust" could pose a greater security risk than a hacker may seem cynical, but a report by the U.S. Treasury Department's Financial Crimes Enforcement Network provides empirical support. That study found that, in 27.5% of suspicious activity reports filed by depository institutions between 2003 and 2009, the identity theft victim knew the suspected thief, who was usually a family member, friend, acquaintance, or an employee working in the victim's home.[28]

4. Gateway to the cloud

Mobile devices can also be viewed as a "gateway to the Cloud." That is, mobile device users are offered a variety of free or low-cost applications, such as Dropbox and Evernote, that allow them to create content and store it, or back it up, using cloud-based storage. While these tools offer great convenience and functionality for consumers, companies must evaluate whether they provide sufficient security before they are used to store company data, especially sensitive personal data, health data, or company trade secrets. Many of the federal and state regulations discussed below impose obligations on companies to: (1) carefully select and oversee their vendors to ensure they are capable of protecting their information; and (2) bind those vendors by contract to safeguard sensitive information. Although these statutes do not specifically address dual-use devices or cloud storage, they extend to sensitive information, regardless of where it is stored. Moreover, as noted below in the discussion of the Stored Communications Act (see Section III.C.2), a company may not have ready access to their data if it is stored with a cloud provider under contract with the employee rather than the employer.

5. Implications of a security breach

These risks can expose organizations to government enforcement actions, civil penalties, and litigation as statutory, regulatory and contractual obligations to safeguard sensitive information become increasingly prevalent. Under the information security regulations (the "Security Rule") promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), hospitals, health care providers, health insurers and self-insured health plans are required to implement technical, physical and administrative safeguards for protected health information (PHI) in electronic form.[29] Notably, the U.S. Department of Health and Human Services, which enforces HIPAA, has recently

28 U.S. Department of Treasury, Financial Crimes Enforcement Network, *Identity Theft: Trends, Patterns and Typologies Reported in Suspicious Activity Reports Filed By Depository Institutions, January 1, 2003 – December 31, 2009*, Oct. 2010, *available at* http://www.fincen.gov/news_room/rp/reports/pdf/ID Theft.pdf, at 4.

29 *See* 45 C.F.R. pts. 160, 162 and 164.

obtained seven-figure settlements in two different matters arising from security breaches.[30] Like HIPAA, the Gramm-Leach-Bliley Act (GLBA) extends protections to information created or received by a "financial institution"–a broadly defined term that includes not only banks but also car dealerships that extend credit and even some travel agencies–in connection with the customer relationship.[31]

Many states have enacted laws that impose information security obligations on businesses that collect or store Social Security numbers, drivers' license numbers, credit and debit card numbers, and financial account numbers. Massachusetts and Oregon, for example, require that such businesses implement a comprehensive, written information security program and provide detailed requirements for implementing the program.[32] Massachusetts' information security regulations specifically address portable devices, requiring encryption of personal information stored on them. Moreover, the Massachusetts Attorney General has recently obtained monetary penalties against businesses that have failed to fulfill information security obligations.[33]

Other states, such as California and Texas, impose a general statutory duty on businesses to safeguard personal information.[34] In addition to these more general requirements, a majority of states have enacted narrower information security laws. At least twenty-nine states, for example, require the secure destruction or protection of personal information in electronic form.[35]

While these statutes and regulations tend to apply only to specific industry sectors or states, their impact has resonated far beyond the businesses directly subject to them. Many of those statutes and regulations, either expressly or implicitly, require companies to carefully screen vendors that handle a company's sensitive personal information–such as, third-party administrators, billing services, insurance brokers, information technology consultants, auditors, accountants and attorneys–and ensure they are capable of providing adequate safeguards for sensitive information. Many of these statutes and regulations also require businesses to bind those vendors, by contract, to implement safeguards to protect this information. Although these regulations may not specifically address dual-use devices or cloud storage vendors, they necessarily apply to sensitive information, regardless of where it is stored.

The ultimate objective of these statutes, regulations and contractual provisions is to reduce the risk of a security breach. Notably, 46 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and Guam have all enacted security breach notification laws. Under these laws, when a business knows, or has reason to believe, that *unencrypted*, computerized, personal information has been acquired by an unauthorized person, the business may have a security breach notification obligation depending on whether the state's notice law also requires that the compromise pose a

30 *See* Phillip L. Gordon, *Finding the Messages to Employers in $1.5M HIPAA Settlement*, Workplace Privacy Counsel (Mar. 14, 2012), *at* http://privacyblog.littler.com/2012/03/articles/hipaa-1/finding-the-messages-to-employers-in-15m-hipaa-settlement/; Phillip L. Gordon, *HHS' One-Two HIPAA Penalty Punch Sends a Message to Employers and Providers*, Workplace Privacy Counsel (Mar. 8, 2011), *at* http://privacyblog.littler.com/2011/03/articles/hipaa-1/hhs-onetwo-hipaa-penalty-punch-sends-a-message-to-employers-and-providers/.

31 15 U.S.C. §§ 6801 – 6809.

32 Mass. Regs. Code tit. 201, §§ 17.03 – 17.04; Or. Rev. Stat. §§ 646A.622.

33 *See* Ellen Giblin, *Massachusetts Extends Reach of Data Protection Regulations*, Workplace Privacy Counsel (May 18, 2011), *at* http://privacyblog.littler.com/2011/05/articles/data-security/massachusetts-extends-reach-of-data-protection-regulations/.

34 *See* Cal. Civ. Code §§ 1798.80 *et seq.*

35 *See* National Conference of State Legislatures, *Data Disposal Laws*, *at* http://www.ncsl.org/issues-research/telecom/data-disposal-laws.aspx.

significant risk of harm to affected individuals. Consequently, if an employee's dual-use device is lost, stolen, hacked, or otherwise subject to unauthorized access, the employer will, at a minimum, be required to evaluate whether notification is necessary unless all personal information stored on the compromised dual-use device is encrypted.

Encryption not only provides a safe harbor from security breach notification requirements, it also is, or may be, required by statute or regulation. As noted above, Massachusetts' information security regulations, for example, require encryption of portable storage media containing personal information.[36] Nevada imposes a similar requirement by statute.[37] The HIPAA Security Rule requires that covered entities at least consider whether encryption of personal health information in electronic form is feasible and, if not, to document the basis for that conclusion.[38] In addition to these legal requirements, encryption often is one of the information security measures that businesses are increasingly imposing by contract on their vendors.

Mitigating the risk of a security breach involving a dual-use device, such as by encrypting the device, is critical given the high cost of a security breach to the affected business. According to one recent study, the average loss resulting from a security breach is $5.5 million, or $194 per lost record containing personal information. The average loss includes $3.01 million in lost business costs, such as an abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill caused by the breach.[39]

B. Record Management Laws and Contractual Obligations

Storing company data on employee-owned devices can also create challenges for compliance with an organization's records management obligations. For example, many states require the secure destruction of certain types of sensitive information. Regulations promulgated under the Fair Credit Reporting Act require the secure destruction of consumer report information. In addition, the standard terms of most confidentiality or non-disclosure agreements and court protective orders obligate parties to securely destroy confidential information obtained from the adverse party. If the records are stored on employee devices or with cloud providers under contract with the employee, compliance with these obligations could be frustrated.

C. The Privacy of Employee Data on Dual-Use Devices

Many employers have become accustomed to the mantra that employees "have no reasonable expectation of privacy" in any information stored on, or transmitted through, the employer's information systems. However, the reverse of that mantra controls when an employer permits its employees to use a dual-use device. Employees *do* have a reasonable expectation of privacy in information stored on a portable device that the employee owns. Indeed, that expectation of privacy is codified by statute.

The federal Computer Fraud and Abuse Act (CFAA) makes it a criminal offense to gain unauthorized access to a computer and permits the recovery of civil damages when the unauthorized access results in damage exceeding

36 Mass. Regs. Code tit. 201, § 17.04(5).

37 Nev. Rev. Stat. 603A.215.

38 *See* 45 C.F.R. pt. 164.312(a)(2), (e)(2).

39 Ponemon Institute, *2011 Cost of Data Breach Study: United States*, *supra* note 23, at 2-3.

$5,000.[40] All 50 states have enacted "computer trespass" laws, which largely parallel the CFAA. These laws also typically are criminal statutes with civil remedies; some of those remedies are generous. At least seven states, for example, allow for statutory damages absent proof of actual harm. [41] It is critical for employers who permit dual-use devices to be aware of these laws.

1. Remotely deleting data from employee devices

One security feature commonly used by employers who permit dual-use devices is a "remote wipe" capability. When activated–typically in response to an employee's report that a device has been lost or stolen–this feature deletes any of the employer's information stored on the dual-use device *as well as* all other information stored on the device.[42] In other words, sending a remote wipe command to an employee's dual-use device typically will result in the deletion of the employee's personal contacts, personal e-mail, photos, videos, books, music, and all other personal information stored on the dual-use device. If the employee has not recently backed up their personal data stored on the dual-use device, the deletion could result in the significant loss of potentially irreplaceable data to the employee. Even if the employer activated the remote wipe command with the intention of destroying only the employer's business information, the employer still could be subject to criminal and civil liability if the employee did not provide prior authorization for deletion of his or her personal items. In fact, Littler is aware of two recent cases where employers have received demand letters from terminated employees whose dual-use devices had been remotely wiped by the employer's IT personnel without the terminated employee's prior authorization.

2. Accessing data stored with online services

The federal Stored Communications Act (SCA) raises a similar, but somewhat different, risk for employers.[43] The SCA prohibits unauthorized access to e-mail stored at an e-mail service provider. Like the CFAA, the SCA is a criminal statute with civil remedies. The decision in *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, L.L.C.*,[44] illustrates how the SCA could be used against an employer who permits dual-use devices. In that case, the employer accessed a former employee's Hotmail account, using the log-in credentials that had been stored on the employer's computer system when the employee accessed the account using his work computer. While accessing the employee's Hotmail account, the employer found an e-mail with a password for the employee's Gmail account and accessed e-mail in that account as well. In a counterclaim against the employer, the former employee obtained summary judgment *in his favor* on his SCA claim.[45] Similarly, and as one example, if an employer uses the employee's dual-use device to access

40 18 U.S.C. § 1030.

41 The event states are as follows: California–Cal. Penal Code § 502(e); Nevada–Nev. Rev. Stat. 205.511; New Jersey - N.J. Stat. Ann. § 2A:38A-3 (2011); Rhode Island - R.I. Gen. Laws § 11-52-6; Vermont–Vt. Stat. Ann. tit. 13, § 4106 (2012); Virginia - Va. Code. Ann. § 18.2-152.12; West Virginia - W. Va. Code Ann. § 61-3C-16 (2011).

42 As noted below, some vendors offer security software that allows a company to create a separate, secured area–commonly called the "sandbox"–on the dual-use device for the storage of company data by the employee. This software typically allows a company to issue a wipe command to only the data stored in the sandbox, leaving untouched the rest of the data stored on the dual-use device. So long as the employee has not stored company data outside of the sandbox, this more limited approach could be employed.

43 18 U.S.C. §2701.

44 *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, L.L.C.*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

45 *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, L.L.C.*, 759 F. Supp. 2d 417 (S.D.N.Y. 2010).

an employee's personal e-mail account, without the employee's prior authorization, the employer may be exposed to similar claims.

The same reasoning likely applies to the many forms of remote, cloud-based storage available to users of mobile devices, such as Dropbox, Google Drive, Evernote, etc. Data stored by an employee with these services may be readily available on the device simply by launching an application because the employee may have saved the username and password in the applications. Companies need to ensure they have the employee's consent before accessing data stored with such services.

Companies also need to be careful about relying on verbal consent from employees, because employees may later claim they did not give consent or that the consent was coerced. For example, in *Pietrylo v. Hillstone Restaurant Group*, a district court upheld a jury verdict and punitive damages against an employer for violating the SCA even despite the employer's argument that it had obtained adequate verbal consent. The employer's managers asked an employee to provide her login credentials for a password-protected online chat forum created and used by a group of employees, including the plaintiffs. The employee complied with the manager's request, and the managers subsequently accessed the forum and terminated the employees who had created it. The plaintiff-employees argued that the disclosure of login credentials had been coerced. After a jury trial, the district court concluded, in response to a post-trial motion to overturn the jury's verdict, that a reasonable jury could find that the employee had been coerced into consenting because the employee had testified that she thought "something bad might happen to her if she didn't consent." Consequently, the evidence supported the jury's finding that the manager's access to the chat room had been unauthorized.

3. Employee's privileged communications

At least one court has held that an employer's ability to secure consent from its employees can only go so far. In *Stengart v. Loving Care Agency, Inc.*,[46] the New Jersey Supreme Court held that a former executive employee had a reasonable expectation of privacy in email exchanged between her and her attorney through her personal, web-based email account, even though the email exchange with her attorney was stored in temporary storage on a company-issued computer. The court rejected the defendant-employer's argument that it had a right to review information contained on company-owned devices (*e.g.*, plaintiff's company-issued laptop), stating, "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."[47] Notably, to date, *Stengart* has not yet been followed in any other jurisdiction.

46 *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (N.J. 2010).

47 *Id.* at ¶ 8. It should be noted that many states disagree with the policy implications of *Stengart*, and instead reason that a properly crafted policy provides informed consent. *See, e.g., Holmes v. Petrovich Development Co., L.L.C.*, 191 Cal. App.4th 1047, 1071 (Cal. Ct. App. 2011) (holding plaintiff had no expectation of privacy in personal email sent on a work computer when plaintiff was notified in writing that her employer could inspect her computer at any time at its discretion and where company computers were monitored to make sure employees were not using them to send personal emails, reasoning: "[T]he e-mails sent via company computer under the circumstances of this case were akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him.")

4. Information employers may not want to see

Employers who access information stored on a dual-use device, even with the employee's authorization, could still be exposed to liability. For example, an employer could view "genetic information" which, under the Genetic Information Non-discrimination Act of 2008 (GINA), employers are generally prohibited from collecting. Under GINA, genetic information includes not only the genetic test results of an employee and the employee's family members, but also the manifestation of a disease or disorder–whether hereditary or not–in an employee's family member to the fourth degree.[48] The employer also could discover information upon which an employer cannot lawfully rely to make an employment decision, such as the fact that the employee who owns the dual-use device has a serious eating disorder or other impairment, which constitutes a disability under the Americans with Disabilities Act (ADA).[49] Even seeing that the employee has an App related to a particular disorder or condition installed on his or her device could reveal this information.

D. Preserving and Collecting Data from Employees' Dual-Use Devices for Litigation Holds and Investigations

The field of e-Discovery continues to grow at a rapid rate, touching upon every aspect of evidence in litigation and information management in the workplace. This trend[50] is not surprising given that reported e-Discovery sanctions cases continue to dominate legal headlines,[51] costs for e-Discovery activities in lawsuits–even small ones–continue to skyrocket, new technologies continue to create unique challenges around preserving, collecting and producing electronic data in litigation, and the Discovery Subcommittee of the Federal Courts Advisory Committee on Civil Rules is once again considering another set of amendments to the Federal Rules of Civil Procedure to specifically address all of these issues (with a specific focus on e-Discovery preservation and sanctions issues).[52]

In addition, as e-Discovery continues to mature, the courts are coming back to one of the most fundamental tenets of litigation: defensibility. Even if evidence is electronic, voluminous or grounded in a novel technology, litigants must be prepared to defend how they identified relevant sources of data, preserved, harvested, culled, reviewed and produced that data, as well as the basis for having it admitted into evidence at trial.

48 42 U.S.C. § 2000ff(3), (4).

49 Garry G. Mathiason, Margaret Hart Edwards, et al., *THE LITTLER TEN: Employment, Labor and Benefit Law Trends for Navigating the New Decade*, Littler Report (Sept. 30, 2010) at 9-13 (Littler Three: The Brave New World of Employment Litigation–e-Discovery, Next Generation Class Actions, Privations of Litigation Through ADR and Virtual Trials), *available at* http://www.littler.com/publication-press/publication/littler-ten-employment-labor-and-benefit-law-trends-navigating-new-dec.

50 For a more detailed discussion of e-Discovery trends and predictions, *see The Littler Ten: Employment, Labor and Benefit Law Trends for Navigating the New Decade*, Littler Three: The Brave New World of Employment Litigation–e-Discovery, Next Generation Class Actions, Privations of Litigation Through ADR and Virtual Trials,at 9 – 13, Sept. 2010.

51 *See E-Discovery 2011 Year in Review*, Law Tech. News, Cecil Lynn, III, Feb. 2012.

52 *See Federal Judicial Advisory Committee Ponders New e-Discovery Rules*, Law Technology News, Mark Michels, Apr. 6, 2012, *available at* http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202548101854&slreturn=1 (last accessed Apr. 12, 2012).

Moreover, despite the fact that certain, baseline e-Discovery standards and litigation support technologies[53] are–seven years after *Zubulake*[54]–"well established,"[55] the field of e-Discovery continues to develop at a rapid pace, especially as data volumes expand exponentially, businesses and individuals alike move to a digital platform, and new sources of technology emerge.

Given this backdrop, it should not be surprising that a BYOD environment implicates a host of e-Discovery challenges. As discussed below, employers must balance the significant practical and legal challenges they will face around identifying, collecting and producing data on/from dual-use devices (of both current and former employees) to meet threshold e-Discovery obligations, with any potential costs savings or other perceived benefits of implementing such a program.

1. Identification of BYOD devices/information

A threshold e-Discovery obligation is to identify and preserve relevant sources of data once the duty to preserve is triggered.[56] In today's digital world, this requires having a thorough understanding of an employer's data infrastructure,[57] which may include things like servers and databases that are generally maintained by the IT department, as well as media and other devices that are issued to individual custodians, like computers, PDAs, phones, etc.

Under a "traditional" model, the IT department issues company-purchased and owned computers, PDAs and other devices to their employees. Not only are the devices homogeneous,[58] they are usually indexed and tracked (including

53 From a vendor/technology standpoint, while certain activities are becoming commoditized (*e.g.*, data processing and hosting services), other areas are rapidly emerging (*e.g.*, predictive coding and advanced search technologies). *See, e.g., Search, Forward: Time for Computer Assisted Coding*, Law Technology News Honorable Andrew J. Peck, Oct. 1, 2011 ("If the hot topic in 2010 [in e-Discovery] was proportionality, this year it is computer-assisted coding, often generically called 'predictive coding. By computer assisted coding, I mean tools (different vendors use different names) that use sophisticated algorithms to enable the computer to determine relevance, based on interaction with (*i.e.*, training by) a human reviewer.").

54 The *Zubulake* line of cases are landmark e-Discovery opinions authored by Judge Shira Scheindlin, considered the "matriarch" of the e-Discovery movement in the United States, that are universally recognized as launching the field of e-Discovery. They include:

Zubulake v. UBS Warburg L.L.C. 217 F.R.D. 309 (S.D.N.Y. May 13, 2003) (*Zubulake I*) (addressing the novel question of to what extent inaccessible electronic data is discoverable and who should pay for its production and setting forth seven factor cost-shifting test);

Zubulake v. UBS Warburg L.L.C., 216 F.R.D. 280 (S.D.N.Y. July 24, 2009) (*Zubulake III*) (applying seven factor cost-shifting test for inaccessible data and holding that the cost to restore back-up tapes should be allocated 75% to defendant and 25% to plaintiff);

Zubulake v. UBS Warburg L.L.C., 220 F.R.D. 212 (S.D.N.Y. Oct. 22, 2003) (*Zubulake IV*) (setting forth both the scope of a litigant's duty to preserve electronic evidence and the consequences for failing to preserve evidence that falls within the scope of that duty); and

Zubulake v. UBS Warburg L.L.C., 229 F.R.D. 422 (S.D.N.Y. July 20, 2004) (*Zubulake V*) (setting forth additional steps that must be taken to ensure compliance with preservation obligations and issuing an adverse inference instruction against defendant as a sanction for failing to meet those obligations, and forewarning in a Postscript: "Now that the key issues have been addressed and national standards are developing, parties and their counsel are fully on notice of their responsibility to preserve and produce electronically stored information").

55 *The Pension Committee of the University of Montreal Pension Plan v. Banc of America Sec. L.L.C.*, 2010 WL 184312, *10 (S.D.N.Y. Jan 15, 2010) (landmark opinion authored by Judge Shira Scheindlin, setting forth new, post-*Zubulake* baseline e-Discovery standards, and issuing an adverse inference instruction against 15 plaintiffs in the case based upon the failure to follow those standards).

56 *Zubulake V*, 229 F.R.D. at 439.

57 *Qualcomm Inc. v. Broadcom Corp.*, 2008 U.S. Dist. LEXIS 911, *31 (S.D. Cal. Jan 7, 2008), *vacated in part on other grounds,* 2008 U.S. Dist. LEXIS 16897 (S.D. Cal. Mar. 5, 2008) ("[F]or the current 'good faith' discovery system to function in the electronic age, attorneys and clients must work together to ensure that both understand how and where electronic documents, records and emails are maintained and to determine how best to locate, review, and produce responsive documents."); *Phoenix Four v. Strategic Resources Corp.*, 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y. 2006) (Counsel "failed in its obligation to locate and timely produce [electronic evidence]... [Counsel] affirms that it engaged in a dialogue with the defendants on the need to locate and gather paper and electronic documents... But counsel's obligation is not confined to a request for documents; the duty is to search for sources of information. It appears that counsel never undertook the more methodical survey of the... Defendants' sources of information...."); *Zubulake v. UBS Warburg L.L.C.*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("[A] party and her counsel must make certain that all sources of potentially relevant information are identified and placed 'on hold'... to do this, counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture... it will also involve communicating with the 'key players' in the litigation, in order to understand how they store information.").

58 Corporate IT departments often strive for commonality and redundancy related to electronic information systems. By limiting the variety of a particular

via "asset tags" identifying the devices as being owned by the employer) by the company's IT department. Then, when litigation hits or a duty to preserve is otherwise triggered, the employer has on hand a current inventory of IT assets that have been issued to individual employees, can quickly determine which of those assets are relevant to the matter at hand, and can take appropriate steps to capture and preserve data on those devices.

Under a BYOD model, or in situations where employees are using unapproved cloud-based services, the employer may have very little, if any, information about where its data is stored. The employer is likewise faced with significant challenges around preserving information from these sources, and may be completely at the mercy of its employees, who have no IT training and oftentimes are not directly involved in litigation activities.

2. Practical challenges of collecting data from dual-use devices

Likewise, when dual-use devices are allowed, an employer's IT department may not have the expertise to defensibly collect data from the variety of devices used by their employees for purposes of litigation. For example, a corporation may have the internal qualifications and resources to forensically copy hard drives formatted with a Microsoft Windows operating system, but may have difficulty making copies of an iPhone or iPad used by an employee under the company's BYOD program.[59]

Likewise, the ability and method for collecting data on dual-use devices may vary greatly depending upon its operating system ("OS") (*e.g.*, Apple iOS, Windows Mobile, Android, Palm, etc.). Indeed, there may even be technical challenges to copying devices that have the same OS, but may not be identical. In fact, the Android operating system is "open source software" which allows software developers and computer manufacturers to alter its code to suit their particular needs and devices. This means that standardized tools may not work on certain devices, and internal IT departments and/or forensic investigators may require additional tools and time to copy and search such devices and they may achieve varying results.

A closed OS like the Apple iOS may also have its own set of challenges. Since only part of the software source code is publicly available and licensed to developers, it may be difficult for commercially available forensic software to keep up with OS updates. These delays can substantially impact an employer's and/or a forensic examiner's ability to copy and search different versions of the same software. In fact, when Apple recently updated its OS, the result, intended or incidental, limited the ability make a physical copy of the device that would be necessary to capture deleted information stored on the device's storage, which may be required in certain lawsuits.

3. A threshold inquiry: does the employer "control" company data on dual-use devices

a. "Possession, custody or control"

Under Rule 34 of the Federal Rules of Civil Procedure (FRCP), a party must produce responsive documents and electronically stored information (ESI) that are in its possession, custody or control. The Rule applies equally to

computer or PDA, IT is able to gain an extensive understanding of a relative few systems and provide more in-depth support to the employees that use them. This less-is-more approach also permits a corporation to more effectively service computers and PDAs using common parts and components.

59 *See e.g., Triple-I Corp. v. Hudson Assoc. Consulting, Inc.,* 2009 U.S. Dist. LEXIS 37447, at *10, n. 8 (D. Kan. May 1, 2009) (noting that both parties should confer to resolve production problems that could be as simple as a bad disk or the difference in the parties' respective computer formats (Mac v. PC).

preservation.[60] The Federal Rules, however, do not define control. Thus, it is necessary to look to court decisions for an interpretation. Just like many other areas in e-Discovery, the federal courts' definition of "control" for purposes of Rule 34 preservation and production obligations differs from circuit to circuit (as discussed below), and often the term "control" does not require that a party have legal ownership or actual physical possession of the information at issue.[61]

As an example, in *Hagerman v. Accenture, L.L.P.*, plaintiffs sought e-mail authored and received by certain of defendant Accenture's employees whose e-mails were stored on a Best Buy server. The court rejected Accenture's argument that Best Buy had exclusive control over the employees' emails. Rather, the court held that "[i]f an Accenture employee with a bestbuy.com e-mail address can access information sent from or received by his or her bestbuy.com e-mail address within his or her normal day-to-day work, then that information is within Accenture's control."[62] Conversely, Rule 34 did not apply to information from the Best Buy server that could not be accessed by an Accenture employee within his or her normal day-to-day activity. As a result, Accenture was required to preserve accessible information on the bestbuy.com server.[63]

In a litigation context, for purposes of complying with preservation and production obligations, the courts within different circuits define "control" over data (which triggers the concomitant duty to preserve and produce it) differently. Thus, a parties' obligation to produce certain information, may depend upon where the matter is litigated. The different definitions of "control" under Rule 34 generally fall into three categories as set forth in the chart below:

Category	Rule 34 Definition of "Control"	Circuit Courts that follow this test
Category 1	A party must produce information that it has the legal right to obtain on demand.	District of Columbia, 1st, 3rd, 6th, 7th, 8th, 9th, and 10th Circuits.[a]
Category 2	A party must produce information that it has the legal right to demand as well as the "right, authority or practical ability" to obtain from a non-party.	2nd, 4th, 5th, and 11th Circuits.[b]
Category 3	In addition to the above, these Circuits require a party to notify its adversary about evidence in the hands of third parties.	1st, 2nd, 6th, and 10th Circuits.[c]

[See endnotes at page 58 for references.]

b. Employer's "control" over employees and their work product

The varying definitions of "control" may matter little when evaluating a company's obligation to obtain work-related information from their employees in discovery. In general, a corporate party is deemed to have control over

60 See *Columbia Pictures Indus. v. Fung*, 2007 U.S. Dist. LEXIS 97676, at * 3 (C.D. Cal. 2007) (holding defendants must preserve data within their possession, custody or control); *See also Caston v. Hoaglin,* 2009 U.S. Dist. LEXIS 49591, at * 8-9 (S.D. Ohio 2009) (denying plaintiff's motion to serve subpoenas on defendant's current employees holding that subpoenas were unnecessary given defendant's control over the documents in the possession of its officers and employees).

61 2011 U.S. Dist. LEXIS 121511 (D. Minn. Oct. 19, 2011).

62 *Id.* at **9-11.

63 *Id., See also Nursing Home Pension Fund v. Oracle Corp.*, 254 F.R.D. 559, 567 (N.D. Cal. 2008) (holding defendants liable for third-party author's spoliation of audio taped interview with defendant's CEO who failed to take efforts to preserve the tapes despite having the ability to do so).

its employees and officers.[64] The rational is that these employees are creating work product in furtherance of their employment and owe a duty to the company to maintain these documents for the corporation's benefit.[65] Accordingly, the employee has no right to use the information for his personal purposes, absent the employer's consent[66] and must surrender the information upon demand absent a transfer of ownership or possession.[67]

As a result, courts may quash as improper a subpoena issued directly to an employee pursuant to Rule 45 of the Federal Rules of Civil Procedure.[68] Instead, courts have advised that a Rule 34 Request for Production for corporate (vs. personal) information is a more appropriate vehicle for production of corporate documents or data, regardless of whether the corporate documents are located in the corporate party's office or the employees' homes.[69] Likewise, courts have extended the same theory of control over corporate documents and data to outside directors who are not company employees, even though they may only conduct sporadic business with the corporation.[70]

Most of the relevant case law concentrates on control over the employee or the company's access to work product. However, there is a void in the case law relating to an employee's exclusive ownership of materials requested by a party in litigation. For example, what happens when a party requests information that resides only on the employee's personal dual-use device and the employee claims the information is purely personal and not subject to their employer's control? Here, a strong argument can be made that the employer does not have "control" over such personal information. The case of *Hatfill v. New York Times Co.*[71] is instructive and provides guidance on how a court may rule on an employee's objection to a demand for production.

In *Hatfill*, the plaintiff brought a defamation action against the New York Times. In discovery, plaintiff requested documents from defendant's employees related to published and unpublished reporting on anthrax attacks. The plaintiff filed a motion to compel interview notes stored on a non-party New York Times reporter's personal flash drive. The flash drive was always in the reporter's personal possession although he regularly attached the drive to computers owned by the newspaper as part of his work duties.

The plaintiff argued that the notes were within the defendant's control regardless of whether the reporter kept the notes on a home or work device and thus the notes must necessarily be produced pursuant to Rule 34.[72] The

64 *Gray v. Faulkner*, 148 F.R.D. 220, 223 (N.D. Ind. 1992) ("A party responding to a Rule 34 production request "cannot furnish only that information within his immediate knowledge or possession; he is under an affirmative duty to seek that information reasonably available to him from his employees, agents, or others subject to his control."); *Herbst v. Able*, 63 F.R.D. 135, 138 (S.D.N.Y. 1972) (holding that corporate employees were within the corporate defendant's control and that defendant must obtain copies of SEC transcripts from the employees).

65 *Riddell Sports, Inc. v. Brooks*, 158 F.R.D. 555, 558-59 (S.D.N.Y. 1994) (holding that corporate officer was subject to the control of the corporate party and had to produce tapes made in furtherance of his role as an officer). *See e.g. Flagg v. City of Detroit*, 252 F.R.D. 346, 353 (E.D. Mich. Aug. 22, 2008) (holding that city defendant had sufficient control over city employees text messages to satisfy production requirement under Rule 34).

66 *In re Grand Jury Subpoenas*, 722 F.2d 981, 986 (2d Cir. 1983) ("The officer creates or handles the records in a representative capacity, not on his own behalf. The records, moreover, do not belong to him but to the organization.").

67 *Id.* ("The contents of the documents, except possibly for any personal notes written on them after the witness ceased to be employed by the company, which might be his own personal non-corporate thoughts, are not protected from disclosure by the Fifth Amendment. ").

68 *Shcaaf v. Smithkline Beecham Corp.,* 233 F.R.D. 451, 455 (S.D.N.Y. 2005) (quashing subpoena issued to employee directly because documents sought was owned by company).

69 *See Flagg v. City of Detroit,* 252 F.R.D. 346, 353-54 (E.D. Mich. 2008) (In lieu of ruling on third-party service provider's motion to quash subpoena for defendant's text messages, court instructed plaintiff to serve Rule 34 request on defendants).

70 *Miniace v. Pacific Martime Ass'n*, 2006 U.S. Dist. LEXIS 17127, at *2 (N.D. Cal. Feb. 13, 2006).

71 *Hatfill v. The New York Times Co.*, 242 F.R.D. 353, 354-55 (E.D.Va. 2006).

72 *Id.* at 355.

newspaper, in turn, argued that the flash drive, and by extension, the reporter's notes, were under the reporter's exclusive control. The court agreed and held that the defendant newspaper formally ceded to its reporter employees any right to possess or control dissemination of notes and unpublished materials. This policy was embedded in the defendant's collective bargaining agreement with the reporters' unions and the court found that the newspaper's policy had a clear substantive purpose and was not an artificial wall created for the purpose of avoiding discovery requests.[73] Accordingly, the newspaper did not have the legal right to obtain the flash drive over the reporter's objection.[74]

The court's decision in *Hatfield* suggests that an employee who stakes an ownership claim must be in sole possession of the device at issue. In addition, the employer would most likely need to disclaim its right to control the data on the device, a proposition that runs contrary to the needs of the employer in many other areas discussed in this Report.

Thus, as a general matter, unless an employer has a clear policy that relinquishes to its employees the employer's ownership right over certain data (like the collective bargaining agreement at issue in *Hatfield*), courts will likely require an employer to preserve, collect, review, and produce relevant corporate information stored on dual-use devices and hold them accountable for failing to do so.

c. Former employees

Courts vary on whether a corporation has an obligation or right to obtain its work-product from a *former* employee.[75] However, a severance package or other economic benefit from the corporation may evidence sufficient post-termination control over the employee to subject the former employee to the production demands of Rule 34.[76] And, as discussed in the Recommendations section below, the use of contracts with employees to address access to company data may be necessary to mitigate other risks.

Even where an employer does not have control over a former employee, some courts require, at a minimum, that the employer at least ask a former employee to search for and produce work-related information from their personal devices before the company can assert that it does not control the information under Rule 34.[77]

4. Additional practical and legal limitations on collecting data on dual-use devices

As an additional practical matter, employees may be reluctant to turn over their dual-use devices to the corporation and even more reluctant to have their employers review the contents of their otherwise personal devices. Imagine a scenario where an employer is sued in federal court because a married-supervisor is accused of having an inappropriate

73 *Id.*

74 *Id.*

75 *Cf. Cache La Poudre Feeds v. Land O'Lakes Feed, Inc.*, 244 F.R.D. 614, 627 (D. Colo. 2007) ("The court is not inclined to penalize a party for failing to approach former employees in an effort to respond to "catch-all" or nearly indecipherable requests for production.") and *Miniace*, 2006 U.S. Dist. LEXIS 17127 at **8 - 9 (no obligation to produce documents from former board member).

76 *See, e.g., In re Folding Carton Antitrust Litigation*, 76 F.R.D. 420, 423 (N.D. Ill. 1977) (suggesting that an employer may have control over documents in the possession of a former employee if that individual is still receiving economic benefits from the employer).

77 *Chevron Corp. v. Salazar*, 275 F.R.D. 437, 448-49 (S.D.N.Y. 2011) ("There is thus no evidence that [former employee] was "'unwilling or unable"' to provide [her employer] with the relevant contents of her Gmail account or that [the employer] lacked the practical ability to acquire it from [employee] despite its being located in her private e-mail account rather than on [employee's] server."); *Export-Import Bank of the United States v. Asia Pulp Co.*, 233 F.R.D. 338 (S.D.N.Y. 2005) (court found no indication that corporation did not have practical means to obtain relevant work-related portions of former employees journal given appeared for his deposition); *McCoy v. Whirlpool Corp.*, 214 F.R.D. 637, 641 (D. Kan. 2003) (holding that defendant must contact former employees to determine whether they were in possession of responsive documents).

sexual relationship with his subordinate, and the subordinate claims that the supervisor's dual-use device contains extensive text and e-mail messages that prove her claims. How willing will that supervisor be to turn over his device? Would his/her consent be truly voluntary? Indeed, can he/she be trusted to adequately preserve that information?[78] Moreover, as discussed above, employers may face civil[79] and criminal[80] penalties for accessing an employee's personal data without their informed consent.

Thus, on the one hand, pursuant to Federal Rule of Civil Procedure 34, courts may find that employers have sufficient "control" over corporate data on dual-use devices and are obligated to preserve, collect, search and produce such relevant information. On the other hand, however, at least in some circumstances, employers may risk liability for reviewing certain information stored on an employee's dual-use device regardless of the employer's policy or the employee's purported consent. As discussed above in the section on The Privacy of Employee Data on Dual-use devices, this may leave the employer in an unwinnable Catch-22 stemming from its BYOD policy.

Likewise, in the litigation context, if dual-use devices are in play, counsel may need to confer with their adversary to reach an agreement to limit discovery in a way that meaningfully protects an employee's right of privacy or applicable privileges. If unsuccessful, the employer could seek a protective order from the court to limit the scope of production.[81] An employer also may need to consider having a court-appointed neutral review dual-use devices if there is a reasonable likelihood that it will contain privileged or protected material.[82]

Finally, a BYOD program may open the door to broader discovery of employees' personal data–at the employers' expense. As a general matter, an employer does not have "control" over or the right to access personal information and data stored on home or personal computers, personal e-mail accounts, personal PDAs and the like.[83] Thus, if an adversary demands such information in discovery, an employer can and should object,[84] especially if an employer has policies in place that mandate employees should not use personal equipment (like personal e-mail accounts and computers) for work and/or to communicate about work-related matters. Yet, if an employer has a BYOD program, and is required to access employees' personal devices for *work* data, the plaintiff may claim that an employees' *personal* data that is also stored on those same devices is fair game. Given the high costs of e-Discovery and the inherent risks

78 *See, e.g., When Custodians Could be Culprits*, N.Y.L.J., Adam Cohen and Maureen O'Neil, Oct. 27, 2008.

79 *See e.g.*, Computer Fraud and Abuse Act ("CFAA")(18 U.S.C. § 1030(g)); Stored Communications Act (SCA 18 U.S.C. § 2707(c); Wiretap Act (18 U.S. C. §2520); *Doe v. City and County of S.F.*, 2011 U.S. Dist. LEXIS 143152, at * * 4-6 (N.D. Cal. 2011) (denying defendant's motion for summary judgment related to allegations that defendant violated her right of privacy and the SCA by reviewing and printing copies of her personal Yahoo! emails while she was away from a company-owned computer); *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, L.L.C.*, 759 F. Supp. 417, 428-29 (granting partial summary judgment concluding that defendants established four violations of the SCA when plaintiffs used a defendant's password to access his personal email account).

80 *See* e.g., CFAA (18 U.S.C. § 1030); SCA (18 U.S.C. § 2701(a); Wiretap Act (18 U.S. C. § 2510 *et. seq.*).

81 *See Nalco Chem. Co. v. Hydro Techs., Inc.*, 148 F.R.D. 608, 619 (E.D.Wis. 1993) (granting defendant employer's application for a protective order holding fingerprints of employees are not in employer's possession, custody or control).

82 *See Flagg*, 252 F.R.D. at 353-54 (ordering initial review of text message *in camera* to identify relevant information and then affording defendant an opportunity to raise objections, "as a means of protecting against disclosure to Plaintiff of irrelevant, privileged, or otherwise non-discoverable materials.").

83 *See In re Grand Jury Subpoenas*, 722 F.2d at 986 (2d Cir. 1983).

84 It is fair game to demand the preservation and production of data from plaintiffs' personal computers, e-mail accounts, PDA's and the like–because plaintiffs themselves own and control them. *See e.g., Electronic Discovery Special Report: Plaintiffs Have Their Own Duty to Preserve*, Paul Weiner, Nat'l L.J., Dec. 19, 2011, *available at* http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202536136818&slreturn=1) (last accessed Apr. 15, 2012). In response to such legitimate demands, however, Plaintiffs often reflexively–and improperly–claim that employers are somehow required to preserve their employees' personal data–which is objectionable as employers do not possess and control such data.

of accessing an employees' private communications, any expansion of an employer's obligations should be avoided. As a practical matter, it may be difficult to narrowly tailor a search to segregate an employee's personal information from his/her BYOD device.

5. Sanctions for failing to preserve

The duty to preserve arises "when the party has notice that the evidence is relevant to litigation *or* when a party should have known that the evidence may be relevant to future litigation."[85] Accordingly, employers must notify their employees of their obligation to preserve, and not to destroy, all potentially relevant information, including unique data on their dual-use devices. Employees should also be informed of the consequences of their deletion or alteration of relevant information or the destruction of their dual-use device to avoid the disclosure of otherwise personal information.

When the employer is put on notice of its preservation obligation, notice may be imputed to its employees.[86] Moreover, under general agency law, an employer may be deemed responsible for the spoliation of relevant evidence by its employees.[87] For example, in *E.I. Du Pont de Nemours & Co. v. Kolon Industries,*[88] the court held that the defendant-employer breached its duty to preserve when key employees deleted files and email items from their work computers after they were issued litigation holds to preserve evidence for litigation. The court specifically rejected the defendants' efforts to disassociate itself from the acts of its executives and employees' spoliation to the company.[89]

Kolon Industries confirms that agency principles may govern a party's responsibility for spoliation committed by its employees.[90] In order for liability to attach, however, the employee must act within the scope of their employment.[91] In *Nucor Corp. v. Bell*,[92] the court refused to hold the defendant-company liable for its employee's destruction of his own personal USB thumb drive that allegedly contained plaintiff's confidential information. The court ruled that the defendant's testimony implied that he destroyed the drive to protect himself (as opposed to his employer). The court also noted that the defendant did not consult with his employer prior to his deletion, indicating that he was acting for his own benefit, and not within the scope of his employment.[93] Thus, an employer who has advised employees of the need to preserve information on their dual-use devices may be insulated from, or at least mitigate, spoliation sanctions if, contrary to the interests of the organization, the employee destroys information to shield themselves, and not their employer, from wrongdoing.

85 *Zubulake v. UBS Warburg L.L.C.*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) ("*Zubulake IV*").

86 *Nat'l Ass'n of Radiation Survivors v. Turnage*, 115 F.R.D. 543, 557 (N.D. Cal. 1987) (imputed knowledge prevents "an agency, corporate officer, or legal department [from shielding] itself from discovery obligations by keeping its employees ignorant."); *cf. New Times v. Arpaio*, 217 Ariz. 533, 541, 177 P.3d 275, 283 (Ariz. App. 2008).

87 *E.I. Du Pont de Nemours & Co. v. Kolon Indus.*, 803 F.Supp. 2d 469, 499 (E.D. Va. 2011); *Victor Stanley Inc. v. Creative Pipe*, Inc., 269 F.R.D. 497, 516 n.23 (D. Md. 2010) ("[A]gency law is directly applicable to a spoliation motion, and the level of culpability of the agent can be imputed to the master."); *Goodman v. Praxiar,* 632 F. Supp. 2d 494, 523 n.16 (D. Md. 2009) ("A party may be held responsible for the spoliation of relevant evidence done by its agents.").

88 *Kolon Indus.*, 803 F. Supp. at 499.

89 *Id.*

90 See also *Valentine v. Mercedes-Benz Credit Corp.*, 1999 U.S. Dist. LEXIS 15378, at *4 (S.D.N.Y. 1999).

91 *Armstrong v. Food Lion, Inc.,* 371 S.C. 271, 276, 639 S.E.2d 50, 52 (2006) ("An act is within the scope of a servant's employment were reasonably necessary to accomplish the purpose of his employment and in furtherance of the master's business.").

92 *Nucor Corp. v. Bell*, 251 F.R.D. 191 (D.S.C. 2008).

93 *Id.* at 196.

The bottom line is that a BYOD program can inject a host of e-Discovery complications into a matter that would not be at issue if a company owned the device, and companies adopting such policies must plan to meet these challenges.

E. Protection of Trade Secret Information on Dual-Use Devices

Prior to the advent of BYOD programs, most employers would have disciplined or terminated an employee who brought their own storage devices into the workplace, or who copied company data onto their personal devices. Now, however, these actions are the intended result of a company BYOD program. The risks to the protection of company trade secrets must be carefully analyzed to ensure these risks are well-managed and balanced against the benefits.

Indeed, even before the current BYOD trend, The Economist magazine reported that during this most recent economic downturn "60 percent of American workers who left their employers [in 2008] took some data with them."[94] Against that backdrop, with employees already demonstrating a willingness to take a company's information when they depart, companies need to carefully manage the BYOD trend or potentially jeopardize their confidential information and trade secrets. These concerns are more heightened when dealing with today's tech-savvy twenty and thirty-something employees.

1. The Uniform Trade Secrets Act

To promote uniformity in commerce, and to help standardize the definition of a "trade secret," 47 states have adopted a version of the Uniform Trade Secrets Act (UTSA).[95] Under the UTSA, the definition of a "trade secret" can apply to "[I]nformation, including a formula, pattern, compilation, program, device, method, technique" in which employers have taken "reasonable measures" under the circumstances to protect the secrecy of the information.[96] Amongst the three states that have not adopted the UTSA–Massachusetts, New York, and Texas–courts from those states have recognized a similar obligation for employers to take reasonable measures under the circumstances to protect the secrecy of their information.[97]

---

94 *Theft and the Downturn: Employers Beware–What Departing Employees Take With Them*, The Economist, Feb. 24, 2009, *available at* http://www.economist.com/node/13171494.

95 Ala. Code § 8-27-1 et seq.; Alaska Stat. § 45.50.940 et seq. Ariz. Rev. Stat. § 44-401 et seq.; Ark. Code Ann. § 4-75-601 et seq.; Cal. Civ. Code § 3426 et seq.; Colo. Rev. Stat. § 7-74-101et seq.; Conn. Gen. Stats. § 35-50 et seq.; Del. Code Ann. tit. 6, § 2001 et seq.; D.C. Code Ann. § 36-401 et seq.; Fla. Stat. § 688.001 et seq.; Ga. Code Ann. § 10-1-761 et seq.; Haw. Rev. Stat. § 482B-1 et seq.; Idaho Code § 48-801 et seq.; [765 Ill. Comp. Stat. § 1065/1 et seq.; Ind. Code § 24-2-3-1 et seq.; Iowa Code § 550.1 et seq.; Kan. Stat. Ann. § 60-3320 et seq.; Ky. Rev. Stat. Ann. § 365.880 et seq.; La. Rev. Stat. Ann. § 1431 et seq.; Me. Rev. Stat. Ann. tit. 10, § 1541 et seq.]; Md. Code Ann., Com. Law § 11-1201 et seq.; Mich. Comp. Laws § 445.1901 et seq.; Minn. Stat. § 325C.01 et seq.; Miss. Code Ann. § 75-26-1 et seq. ; Mo. Rev. Stat. § 417.450 et seq.; Mont. Code Ann. § 30-14-401 et seq.; Neb. Rev. Stat. § 87-501 et seq.; Nev. Rev. Stat. § 600A.010 et seq.; N.H. Rev. Stat. Ann. § 350-B:1 et seq.; N.J. Stats. § 56:15-1 et seq.; N.M. Stat. Ann. § 57-3A-1 et seq.; N.C. Gen. Stat. § 66-152 et seq.; N.D. Cent. Code § 47-25.1 et seq.; Ohio Rev. Code Ann. § 1333.61 et seq.; Okla. Stat. tit. 78, § 85 et seq.; Or. Rev. Stat. §646.461 et seq.; 12 Pa. Cons. Stat. § 5301 et seq.; R.I. Gen. Laws § 6-41-1 et seq.; S.C. Code Ann. § 39-8-10 et seq.; S.D. Codified Laws § 37-29-1 et seq.; Tenn. Code Ann. § 47-25-1701 et seq.; Utah Code Ann. § 13-24-1 et seq.; Vt. Stat. Ann. tit. 9, § 4601 et seq.; Va. Code Ann. § 59.1-336 et seq. Wash. Rev. Code § 19.108.010 et seq.; W. Va. Code § 47-22-1 et seq.; Wis. Stat. § 134.90 et seq.; Wyo. Stat. Ann. § 40-24-101 et seq.

96 The Model Uniform Trade Secrets Act as proposed by the National Conference of Commissioners on Uniform State Laws defines "trade secret" in Section 1(4) as:

> Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
>
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Uniform Trade Secrets Act § 1(4) (1979). It is also important to note that several states have modified the definition of a "trade secret."

97 New York has not enacted any civil or criminal statutes defining trade secrets, and New York courts follow the common law and the definition of "trade secret" found in the Restatement of Torts § 757, comment b. *Ashland Mgmt. v. Janien*, 82 N.Y.2d 395, 407, 624 N.E.2d 1007, 1013 (1997).

The obvious risk to employers who do not take reasonable measures to manage BYOD policies is that they could undermine their ability to protect trade secret information. And this failure to take adequate measures to protect confidential information and trade secrets could jeopardize a company's intellectual property. Nonetheless, according to a February 2012 study by the Ponemon Institute, "organizations often do not know if and what kind of data is leaving their networks through non-secure mobile devices."[98]

2. Reasonable measures to protect trade secrets in a BYOD environment

The best practice for companies that deal in highly confidential intellectual property may be to eliminate BYOD devices from the workplace entirely, or at least disallow the practice for employees who work with information the company considers its trade secrets or highly confidential. Instead, if new smartphones and tablets are necessary, or desired, then the company should consider purchasing them for the employees to ensure the company retains ownership and a practical level of control over the devices and the data stored on them.

However, for the many organizations that have already adopted BYOD policies and permitted dual-use devices within the workplace, the problem becomes how best to manage the BYOD situation. To address concerns regarding BYOD practices, companies should consider a multi-tiered approach, which includes updating confidentiality agreements, taking practical steps within the workplace to safeguard confidential information and trade secrets, and relying upon post-termination efforts to preserve (if necessary) and then delete company information from departing employees' dual-use devices.

3. Confidentiality agreements

Under the UTSA, one of the well-recognized best practices to protect the secrecy of information is the use of confidentiality agreements.[99] While having a policy or non-contractual document regarding confidentiality is helpful, the more recognized practice is to enter into confidentiality agreements with employees.[100] An agreement with an employee has the added benefit of clearly being enforceable after the employee departs the company, while it is not clear that a company policy would continue to apply.

States have a varying patchwork of rulings regarding whether continued employment is sufficient consideration for such restrictive covenants, and modifications and upgrades to existing agreements should be made with the advice

Texas has not enacted any civil statute defining trade secrets and, in civil matters, Texas courts generally follow the definition of "trade secret" found in the Restatement of Torts §757, comment b. *Chapa v. Garcia*, 848 S.W.2d 667, 671 (Tex. 1992). However, Texas has enacted criminal statutes defining trade secrets and imposing felony liability for the theft, copying, communicating or transmitting of a trade secret without the owner's consent. Tex. Penal Code Ann. § 31.05.

Massachusetts has not enacted any version of the Uniform Trade Secrets Act, but it has enacted a civil statute imposing tort liability for the misappropriation of trade secrets. Mass. Gen. Laws ch. 93, § 42. Massachusetts also has enacted a criminal statute that defines the term "trade secret" and imposes criminal sanctions for the misappropriation or theft of trade secrets. Mass. Gen. Laws ch. 266, § 30. The civil statute borrows the criminal statute's definition of trade secret. Mass. Gen. Laws ch. 93, § 42.

98 *Global Study on Mobility Risks, Survey of IT & IT Security Practictioners*, Ponemon Institute, Feb. 2012 at 9.

99 However, companies with unionized employees must use care when using arbitration clauses, because a Company cannot contract directly with employees over terms and conditions of employment that are a mandatory subject of bargaining. *Int'l Union, United Auto., Aircraft, & Agricultural Implement Workers of America*, Local 180 v. J.I. Case Co., 26 N.W.2d 305, 310 (Wis. 1947); see also *General Elec. Co.*, 150 N.L.R.B. 192 ("The employer's statutory obligation is to deal with the employees through the union, and not with the union through the employees.").

100 See *Metropolitan Foods d/b/a Driscoll Foods v. Kelsch*, No.: 11-3306 (D.N.J. Feb. 12, 2012).

of counsel.[101] Consideration is, however, a flexible concept, and granting the employee the ability to use their personal device for work purposes would likely be considered adequate consideration for the commitments the employer seeks regarding its confidential data that may be stored on the devices.

4. Practical measures

When reviewing an employer's efforts to take reasonable measures to protect its confidential information and trade secrets, courts also review what practical measures were deployed in the workplace to maintain the secrecy of the information.[102] Examples of some of these steps are included in the Recommendations section (Section V.) at the end of this Littler Report.

101 McDonald and Lichty, *Drafting and Enforcing Covenants Not to Compete*, at 131-39 (BNA 2009).

102 Alabama:

Allied Supply Co. v. Brown, 585 So.2d 33, 35-36 (Ala. 1991) (customer and vendor lists were not subject of reasonable efforts to preserve and maintain secrecy, and thus did not constitute trade secrets, where at least 10 employees had free access to the information, the employees did not have written employment agreements or any noncompetition agreements, the information was not identified as "confidential," numerous copies of the information existed, and employees frequently took the information home with them).

Alagold Corp. v. Freeman, 20 F. Supp. 2d 1305, 1315-16 (M.D. Ala. 1998) (information was not subject of reasonable efforts to maintain secrecy, and thus not a protectable trade secret, where employees had free access to the information, information was stored in unlocked cabinets, the information was not identified as confidential, and employer did not maintain nondisclosure or noncompetition agreements with employees).

California:

Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514, 1523 (1997) (customer list was subject of reasonable efforts to preserve secrecy where it was stored on a computer with restricted access, employer required employee to execute employment agreement expressly referring to such information as confidential, and employer's employee handbook included provisions prohibiting the disclosure or use of such confidential information).

Connecticut:

Charter Oak Lending Group, L.L.C. v. August, 127 Conn. App. 428, 437-39 (2011) (customer list was subject to reasonable efforts to maintain secrecy where, among other things, employer maintained computer security in that information was encrypted and password protected, physical security was maintained by way of alarm system, employee handbooks identified such information as confidential, employees were not permitted to take information with them after departing employer).

Florida:

Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Dunn, 191 F. Supp. 2d 1346, 1351 (M.D. Fla. 2002) (employer established customer list information was subject of reasonable efforts to maintain secrecy and entitled to trade secret protection where employees signed nonsolicitation and nondisclosure agreements).

Minnesota:

Nordale, Inc. v. Samsco, Inc., 830 F. Supp. 1263, 1274 (D. Minn. 1993) (despite employer's conclusory claims that it treated its information as confidential and restricted access to those on a need-to-know basis, the court found no evidence to support such claims and held the employer failed to make reasonable efforts to maintain secrecy of information, and the information thus did not constitute a trade secret, where the employer failed to put individuals on notice regarding the confidentiality of such information and did not require individuals to sign confidentiality agreements).

Aries Information Systems, Inc. v. Pacific Mgmt. Sys. Corp., 366 N.W.2d 366, 369 (Minn. Ct. App. 1985) (employer took reasonable steps to maintain secrecy of information where it required employees to sign confidentiality agreements).

Missouri:

Conseco Finance Servicing Corp. v. North American Mtg. Co., 381 F.3d 811, 819 (8th Cir. 2004) (applying Missouri law; employer took reasonable steps to maintain secrecy of information where all employees recognized the information was confidential and not to be disclosed and employer's employee handbook identified such information as "strictly confidential").

Pennsylvania:

A.M. Skier Agency, Inc. v. Gold, 747 A.2d 936, 941 (Pa. Super. Ct. 2000) (employer made reasonable efforts to preserve secrecy of client information where the information was password protected and employer's employee handbook included provision stating that employer owned such information).

Virginia:

Dionne v. Southeast Foam Converting & Packaging, Inc., 240 Va. 297, 301-303, 397 S.E.2d 110, 112-113 (1990) (information was subject of reasonable efforts to maintain secrecy where employer required employees, suppliers, customers, contractors, and visitors to employer's manufacturing plant to execute confidentiality agreements).

Washington:

Precision Moulding & Frame, Inc. v. Simpson Door Co., 77 Wash. App. 20, 27-28, 888 P.2d 1239 (1995) (information found not to be subject of reasonable efforts to maintain secrecy, and thus not a trade secret, where no agreement existed to preserve the confidentiality of the information and the person from whom such information was acquired took no steps to preserve its secrecy).

5. Proving misappropriation of trade secret information

The UTSA imposes liability where a "misappropriation" of trade secrets occurs.[103] A "misappropriation" requires the "use" or "disclosure" of the trade secret information or the "acquisition" by "improper means" of the trade secret. "Improper means" includes "theft," "bribery," violations of confidentiality obligations, and "espionage."[104]

BYOD policies may make it more challenging for an employer to prove "misappropriation" under this standard, because the employee was permitted to store the company's trade secrets on the employee's dual-use device.[105] As a result, the focus will more likely be upon the improper "use" or "disclosure" of the alleged trade secret.

But finding evidence of such use can be more challenging when BYOD policies are in effect. Under circumstances where the employer owns the computing devices, a former employee's devices can easily be gathered and analyzed for evidence of a "misappropriation." Quite often it is important to proceed quickly with the litigation process where the employer suspects a "misappropriation" has occurred. Yet these steps can be much more challenging if the employer does not own the device, and the employee has already left the company's employ.

First, the employer will not likely obtain access to the employee's smartphone or tablet without threatening or commencing a lawsuit. Once a lawsuit is commenced, the employer may seek to analyze and review the employee's smartphone and tablet. Before that process commences, the employer will likely need to serve formal discovery and enter into a protective order with the employee, which will limit the employer's access to the employee's private files and records. Negotiating a protective order can be time-consuming and expensive. Likewise, serving written discovery to collect and analyze an employee's devices adds to the expenses incurred by the employer. And, because employees

---

103 The Model Uniform Trade Secrets Act defines "Misappropriation" in Section 1(2) to mean:

(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the trade secret; or

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was

(I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

Uniform Trade Secrets Act § 1(2) (1979).

104 The Model Uniform Trade Secrets Act defines "improper means" in Section 1(1) as including "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." Uniform Trade Secrets Act § 1(1) (1979).

105 *USI Ins. Servs. L.L.C. v. Miner*, 801 F. Supp. 2d 175, 196, n. 21 (S.D.N.Y. 2011) (evidence of misappropriation where employee uses work e-mail address to e-mail file to personal e-mail account); *EMC Corp. v. Arturi*, 2010 U.S. Dist. LEXIS 132621, at *18 (D. Mass. Dec. 15, 2010) (former employee took with him from former employer "a thumb drive containing thousands of [the former employer's] confidential files"); *ABT, Inc. v. Juszczyk*, 2010 U.S. Dist. LEXIS 91613, at **10-11, 17 (W.D.N.C. Aug. 9, 2010) (misappropriation established where former employee "copied confidential, proprietary, and trade secret information maintained on his [work] laptop and belonging to [his former employer] to his personal Seagate external hard drive"); *Haldeman-Homme, Inc. v. Donahoe*, 2006 U.S. Dist. LEXIS 63450, at **12-13 (D. Minn. Sept. 5, 2006) (former employee sent confidential information to his personal, home e-mail address); *Liebert Corp. v. Mazur*, 357 Ill.App.3d 265, 281-282 (2005) (former employee downloaded 60 megabytes of data from former employer's limited access server to his home computer); *LeJeune v. Coin Acceptors, Inc.*, 381 Md. 288, 313-15, 849 A.2d 451 (2004) (misappropriation by "improper means" where employee copied his employer's computer files to a CD); *Rapid Temps, Inc. v. Lamon*, 144 N.M. 804, 809-10 (N.M. Ct. App. 2008) (misappropriation established where employee copied former employer's confidential information to her home computer and zip drives); *but see Applogix Dev. Group, Inc. v. Dallas Cent. Appraisal Dist.*, 2006 U.S. Dist. LEXIS 61564, at *16 (N.D. Tex. Aug. 29, 2006) ("That a former employee copies his personal hard drive before he departs does not transform those files into valuable, proprietary data guarded to the requisite degree to meet the trade secret test. A showing must still be made that a specified trade secret exists.").

may back-up their devices on their home computer or a cloud-based service, an employer can find itself expending considerable legal and computer forensic resources to gather and review information from multiple sources.

F. Use of Dual-Use Devices By Contingent Workers

In addition to the risks to company information when employees depart, companies should also focus on the risks of workers who join their organization and may bring with them confidential or trade secret data from their prior employment. This problem is especially acute in the case of contingent workers, who, due to their itinerant nature, may pass through any number of companies in a short period of time or may work for more than one company simultaneously. If a contingent worker's former employer also had a BYOD policy, the new company should take steps to prevent lawsuits by the former employer by ensuring that the contingent worker's former employer's confidential or trade secret information does not find its way into the new company's systems through the worker's dual-use device or other storage media.

1. General considerations

The kinds of contingent workers that present special issues in the BYOD context are principally independent contractors and temporary employees assigned by staffing firms. However, for purposes of BYOD issues, it also makes sense to consider as part of the contingent workforce any retained outside consultants from established firms who, unlike temporary employees and individual contractors, are not supervised by internal staff but who nevertheless work on a company's premises with generous access to company information and computing resources.

A common practice that is similar to the outside consultant arrangement is the on-site supervisor placed by a staffing firm to manage the relationship with the hiring company and a large number of temporary employees assigned to a site (usually 50 or more). Companies frequently provide such on-site coordinators the same office space, integrated communications, and other tools they provide to employees, but in many situations, this access is provided without the usual protections offered by company policies or employee contracts.

Although Professional Employer Organizations (PEOs) are usually grouped with staffing firms, the workers that they payroll and administer for their customers are not independent or transient and are therefore not really contingent in the way we mean it in this Report. Workers provided through a PEO are regarded as the customers' own main workforce, and PEOs typically manage each customer's entire workforce, so the BYOD issues with PEO situations are the same as with companies' direct workforces. Even so, the company should coordinate with its PEO to ensure that, between the two employer firms, a complete and consistent BYOD policy is promulgated to the workforce.

A company's rights and protections with regard to BYOD issues in the contingent workforce depend principally on the language of their contracts with the independent contractors or with the staffing firms and consulting organizations that place them. Regrettably, many of these contracts will be documented on the vendor's form agreements, which tend to omit many of the protections a company may need and which disclaim or severely limit the vendor's liability. A further problem is that the employment agreements or other contracts, if any, that the vendors have with the individuals they assign may not fully position the vendors to support a company's rights vis-à-vis the contingent workers.

Consequently, attention should be paid to both levels of contracts. Companies are also well advised to manage this issue by creating agreements with the individual contingent workers to address these gaps.

2. Individual onboarding considerations

Most companies have elaborate processes for requiring their new employees to sign employment agreements and other documents that set up rules, obligations, and protections for the company. But contingent workers typically do not go through this process. They are often brought in directly by operating units concerned only with their immediate operational needs, without the involvement or even the knowledge of Human Resources, the legal department, or other gatekeepers, thereby bypassing established HR processes that deal with:

- Preservation of the company's intellectual property.
- Return of company property.
- Management of passwords and user IDs in company systems and compliance with the company's broader information protection policies and procedures.
- Protection of confidential information and trade secret information.
- Adherence to ethical and behavioral codes.
- Disclaimers of entitlement to company benefit plans and fringe benefit policies, including those affecting computers and communications devices.
- Regulation of use of company IT systems.

Ironically, this risk even extends to staffing agencies with respect to their own risks as operating companies. They may lack protective documentation when they draft members of their own temporary employee population to perform jobs in their internal staffing operations. This is the so-called "in-house temporary" phenomenon.

Contingent workers who use dual-use devices also create another, perhaps even greater, risk for companies. They may be simultaneously working for other companies and will most certainly work for other businesses when their current engagements end. Thus, procedures to ensure that data are removed from the devices of these contingent workers before their engagements end are critical.

IV. BEHAVIOR-RELATED CHALLENGES OF BYOD

A. Performance Management

The overall key to managing employee performance and productivity is to set clear values and expectations and then hold employees accountable. For employers with BYOD programs, drawing lines around what is and is not appropriate use of dual devices is challenging, but vital. Employers should revise their policies to establish the appropriate values and expectations in reaction to new issues created by dual-use devices; it is imperative that employers effectively educate employees on the company's rules regarding personal devices and their implications for and interactions with corporate values.

Many employers are finding gaps in policies and procedures regarding appropriate use of technology because the rules were based on the functionality of devices that existed when the policies and procedures were initially drafted. Today's smartphones and tablets are not just cellphones. They are cameras, voice recorders, scanners, calendars, clocks, navigation systems, gambling devices, portable movie theatres, bookstores, magazine racks, games, and computers. Policies and procedures should no longer be specific to the hardware but instead should address the broad range of activities for which these devices can be used.

Employers typically refrain from developing policies that attempt to regulate off-the-clock behavior, but when employees are using personal devices sanctioned by the employer for use in the course and scope of employment, the lines between work and personal time blurs. When looking at regulating what employees can do with a smartphone, employers must be careful not to infringe on personal "freedoms," while also not inadvertently creating an environment that easily allows the entry of offensive material into the workplace. Several years ago, an employer in South Carolina terminated an employee who refused to take his confederate flag sticker off of his personal lunch box. Ultimately, the Fourth Circuit found that the employer had a legitimate, nondiscriminatory basis for terminating the employee.[106] Dual-use devices may be the new "lunch box" for employers, and employers should craft new policies and procedures that anticipate the risks associated with allowing the devices in the workplace.

Moreover, given that employees may use their personal devices for conduct outside of the workplace that would not be permitted on work premises, there is a significant likelihood those activities may bleed over into the workplace. For example, the icons for some Apps or photographs stored on the device may not be suitable for work, yet the employee will be using that same device to conduct work. Employers will need to find ways to deal with the consequences of this blurring of the lines.

B. Equal Employment Opportunity & Dual-Use Devices

One area where the "lunchbox" analogy may be tested is the issue of harassment claims based upon the content of an employee's dual-use device. Federal, state and local law requires employers to provide their employees and prospective employees with equal employment opportunities (EEO) in the terms and conditions of their employment. More specifically, federal EEO laws prohibit discrimination and harassment based on race, color, national origin, ancestry,

106 *Dixon v. Coburg Dairy, Inc.* 330 F.3d 250 (4th Cir. 2003).

sex, and religion;[107] veteran status,[108] genetic information,[109] pregnancy,[110] age;[111] physical or mental disability;[112] and require reasonable accommodation of qualified people with disabilities.[113] Some states and local governments are even more expansive, *e.g.*, prohibiting discrimination based on sexual orientation,[114] and the EEOC recently recognized a claim of employment discrimination based on gender identity, change of sex and/or transgender status under Title VII.[115] Federal, state and local EEO laws also prohibit retaliation against employees based on their opposition to unlawful discrimination or harassment or participation in any investigation, proceeding, or hearing concerning such a practice.[116] Most employers embody these legal prohibitions in their own employment policies.

The use of personal devices for work purposes creates two primary EEO challenges for employers seeking to follow the law. One involves preventing and remediating harassment based on a hostile environment. The other involves reasonably accommodating qualified persons with disabilities.

1. Unlawful harassment based on the existence of a hostile work environment

Employers must provide their employees with a workplace free of unlawful harassment, including harassment based on the existence of a hostile work environment. An employee may establish the existence of such an environment if she shows that specific conduct created an environment that a reasonable person would find hostile and one that the victim actually perceived as abusive. Sexual harassment is one form of harassment, but harassment claims may be based upon any other protected characteristic. Relevant factors for determining the existence of a hostile work environment include the frequency of the conduct, its severity, whether it is physically threatening or humiliating, and whether it unreasonably interferes with the employee's work performance.

As noted above, some employees who use their own devices for work may use their personal devices for activity and content that violate company EEO policies. They may not observe carefully enough the boundaries between conduct that is private and conduct that may create a hostile environment for coworkers. For instance, an employee who brings his personal smartphone to use on the job may believe his ownership of the device itself entitles him to watch pornographic videos with others in the workplace.

Likewise, an employee may believe that using online resources places him or her beyond the employer's purview and insulates the employer and employee from liability. Two cases underscore how mistaken this view can be. In *Blakey v. Continental Airlines, Inc.*,[117] a female pilot complained of a sexually hostile work environment based upon the content

107 Title VII of the Civil Rights Act of 1964 (Title VII), 42 U.S.C. §§ 2000e *et seq.*

108 Uniformed Services Employment and Reemployment Rights Act, 38 U.S.C. §§ 4301 *et seq.*

109 Genetic Nondiscrimination Act, 42 U.S.C. §§ 2000ff *et seq.*

110 Pregnancy Discrimination Act of 1978, 42 U.S.C. § 2000e(k).

111 Age Discrimination in Employment Act of 1967, 29 U.S.C. §§ 621 *et seq.*

112 Rehabilitation Act of 1973 (Rehab Act), 29 U.S.C. §§ 701 *et seq.;* Americans with Disabilities Act of 1990 (ADA), 42 U.S.C. §§ 12101 *et seq.*

113 ADA, 42 U.S.C. §§ 12101 *et seq.*

114 *See, e.g.,* Colo. Rev. Stat. §§ 24-34-401(7.5), -402(1).

115 *Macy v. Holder*, [EEOC Decision in Appeal No. 0120120821] and discussion in Littler's DC Employment Law Blog *available at* http://www.dcemploymentlawupdate.com/2012/04/articles/eeoc-1/eeoc-finds-claim-of-discrimination-based-on-gender-identity-transgender-status-is-cognizable-under-title-vii/.

116 *See, e.g.,* 42 U.S.C. § 2000e-3(a) (Title VII).

117 751 A.2d 538 (N. J. 2000).

on an Internet message board used by pilots and crew members to exchange personal and business information. Some of the postings on the board included sexual comments about the female pilot, and she sued for sexual harassment. The New Jersey Supreme Court had to consider whether, as plaintiff argued, the message board was an extension of the workplace, much like a bar where employees gathered after work. The court rejected Continental's argument that it did not control the message board and consequently, had no control over its harassing content. Instead, the court found that the company failed to take remedial action when it became aware of potential harassment.

Similarly, in *Espinoza v. County of Orange,*[118] the California Court of Appeals recently upheld a jury verdict based on a state-law claim of disability harassment based on the employer's failure to take adequate steps after learning of inappropriate online and workplace conduct toward the plaintiff. In that case, the plaintiff was a probation department employee. From birth, his right hand had two small stubs but had no fingers or thumb. His coworkers created two blogs outside of work in which they posted derogatory, disability-related comments about him, including references to his hand (and him) as "the claw."[119] Someone told the plaintiff about the blogs, and he read them daily for about six weeks before reporting the 220 pages of comments to his supervisors. The plaintiff alleged the employer emailed employees to request that they shut down the blog, but the blog continued for another eight weeks, and the workplace harassment did not stop. The employer shut down access to workplace computers through generic logins but not through personal logins of employees even though that would have been easy to do. Plaintiff gave the employer names of those coworkers whom he believed were posting the comments, but the employer did not interview him or them. The plaintiff filed suit, went to trial and was awarded $820,000, including $500,000 in emotional distress damages. On appeal, the employer relied on *Blakey,* asserting that the blogs were not "'so closely related to the workplace environment and beneficial to [the employer] that a continuation of harassment on the forum should be regarded as part of the workplace.'"[120] The appeals court disagreed, noting that *Blakey* also taught that "the employer has a duty to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace...."[121] This was especially true because the employer's investigation revealed that the co-employees accessed the blog on workplace computers, that the blog entries referred both directly and indirectly to plaintiff and referred to work-related issues, and that the supervisors believed employees were posting because they sent emails to them because of the blog entries.

If *Blakey* recognized that conduct outside the traditional office could create employer liability for harassment, and *Espinoza* applied it even in the absence of clear benefits of the harassment to the employer, *Guardian Civic League v. Philadelphia Police Dept*.[122] demonstrated that the scope of potential liability for such conduct could be substantial. In that case, two police fraternal and a civil rights organization filed suit in 2009 against the Philadelphia Police Department and others on behalf of all African American police officers for hostile environment based upon race,

118 Case No. G043067 (consol. with G043345) (Cal. App. 4th App. Dist. Feb. 9, 2012) (unpublished).

119 *Id.* at 5.

120 *Id.* at 12 (quoting *Blakey*, 751 A.2d at 543).

121 *Id.* (quoting *Blakey*, 751 A.2d at 552).

122 Civil Action No. 2:09-cv-03148-CMR (E.D. Pa. filed July 15, 2009).

race discrimination and conspiracy to commit civil rights violations. The plaintiff alleged that the police department permitted, participated in, encouraged and let its computers be used in the operation by a police sergeant of a website called "Domelights," on which he and other active duty white police officers anonymously posted racist and offensive content about African American officers and then ignored complaints about that content.[123] The parties settled the case in 2011. Although the police never admitted liability, the settlement provided more than $170,000 in economic relief for plaintiffs, as well as attorneys' fees, consultant fees and training and a commitment to a variety of remedial and preventive non-economic measures.[124]

The *Blakey* and *Espinoza* courts concluded, and the plaintiffs *Guardian Civic League* plaintiffs alleged, that online activity by employees could create vicarious liability for employers for the racially hostile work environments resulting from that activity. These cases help to demonstrate that employers that permit employees to use their own technology for work purposes without exercising at least some control over those devices may permit those employees to extend the scope of their workplace and more easily create, access and use content that become an integral part of their workplace.

Exercising control over how employees use their personal devices in the workplace or on work time is essential to reducing risk for creation or maintenance of a hostile work environment. The most expeditious ways of doing this are prohibiting the use of those devices for any work purposes, establishing written policies limiting the use of private devices and websites outside the workplace to avoid harassing other employees, and blocking access to and sharing of certain offensive content. However, employers that have decided to allow dual-use devices, should consider the following:

- Crafting and training supervisors and employees on a policy concerning the use and misuse of all electronic resources during work time and on work premises.
- Modifying existing policies to ensure that they cover harassment by coworkers and others for off-duty conduct that creates a hostile work environment.
- Training all employees concerning the proper use/misuse of dual-use devices[125].

2. Failure to reasonably accommodate qualified persons with disabilities

There are circumstances when an employer may be obligated to accommodate an employee who brings their own device to work with additional assistive technology that might help that employee perform the essential functions of a job.

The ADA requires employers to provide current or prospective employees who are qualified individuals with physical or mental disabilities with reasonable accommodations to permit them to perform the essential functions of a job unless doing so would cause undue hardship.[126] A qualified person with a disability is able to perform a job's

123 *Id.,* Complaint (E.D. Pa. filed July 16, 2009) (alleging claims under 42 U.S.C. §§ 1981, 1983, 1985 *et seq.*).

124 *See generally* Stipulation of Dismissal, Civil Action No. 2:09-cv-03148-CMR (E.D. Pa. filed June 29, 2011 [Docket No. 48].

125 For further suggestions about how to regulate dual-use technology, see *Managing Employees' Use of Personal SmartPhones and Tablets for Work* in Littler's Workplace Privacy Blog.

126 42 U.S.C. § 12112(a), (b)(5)(A) (1994). *See US Airways, Inc.*, 535 U.S. at 400. ("An ineffective modification or adjustment will not accommodate a disabled

essential functions with or without a reasonable accommodation. Under the ADA, employers must engage in an interactive process in which it has ongoing, good faith communication with employees about their known disabilities. Through the interactive process, the current or prospective employee may clarify whether "any change in the work environment or in the way things are customarily done" would allow the individual to perform the essential functions of the job.[127] A modification or adjustment is "reasonable" if it appears to be "feasible" or "plausible."[128] Where several reasonable accommodations are possible, the employer has discretion as to which option it chooses to implement.[129] The employer need not choose the "best" accommodation or the accommodation the employee seeks. Rather, "the employer has the ultimate discretion to choose between effective accommodations, and may choose the less expensive accommodation or the one which is easier for it to provide."[130]

Employees who use their own devices pursuant to a BYOD policy may seek an accommodation to the extent their device supplies them with some form of assistive technology that helps them perform the essential function of their job.[131] For example, an employer may be required to pay for assistive software for the employee's device or otherwise pay for the employee's device if it contains some type of assistive function necessary for a qualified employee to perform the essential function of their job. In *Rojek v. Catholic Charities of Jackson, Inc.,*[132] for example, a blind applicant for a social work position requested, among other things, a special document reader to do the essential functions of her job. The court held that the applicant could go to trial over whether the request was reasonable. Similarly, in *Herring v. Department of Social and Health Services*,[133] a blind employee requested the use of an eyesight assistance viewer to review a training manual, but the employer claimed that the assistive technology was unreasonable because it was too expensive. A jury found for the employee and the court upheld the jury award because there was enough evidence to show that the requested accommodation was reasonable and the employer failed to accommodate her.

In *Rojek* and *Herring*, the employers relied heavily on the undue hardship[134] defense to the general obligation to accommodate a qualified person with a disability. But generalized conclusions about undue hardship are insufficient.

individual's limitations.") (emphasis original). Many states, such as California through its Fair Employment and Housing Act, impose comparable obligations. CAL. GOV'T CODE § 12900, *et seq.*

127 29 C.F.R. pt. 1630 app. § 1630.2(o) (1997).

128 *See US Airways, Inc. v. Barnett*, 535 U.S. 391, 401-02 (2002); *Monette v. Electronic Data Sys. Corp.*, 90 F.3d 1173, 1184 (6th Cir. 1996); *Vande Zande v. Wisconsin Dep't of Admin.*, 44 F.3d 538, 543 (7th Cir. 1995).

129 *See Scott v. Montgomery County Gov't*, 164 F. Supp. 2d 502 (D. Md. 2001).

130 See *Salmon v. West Clark Community Schools*, 64 F. Supp. 2d 850, (S.D. Ind. 1999); *Allen v. Georgia Power Co.*, 980 F. Supp. 470 (N.D. Ga. 1997); *Scott v. Montgomery County Gov't*, 164 F. Supp. 2d 502, (D. Md. 2001); *Kuehl v. Wal-Mart Stores, Inc.*, 909 F. Supp. 794, (D. Colo. 1995); *Salmon v. West Clark Community Schools*, 64 F. Supp. 2d 850, (S.D. Ind. 1999); *Zimmerman v. General Motors, Delphi Energy & Engine Mgmnt Sys. Div.*, 959 F. Supp. 1393 (D. Kan. 1997).

131 *See* 29 C.F.R. § 1630.2(o)(2)(i-ii) (1997).

132 2010 U.S. Dist. LEXIS 52056 (E.D. Mich., May 27, 2010).

133 81 Wn. App. 1 (1996).

134 The Model Jury Instructions from the Employment and Labor Relations Law Committee of the American Bar Association define "undue hardship" as:

> significant difficulty or expense incurred by the defendant when considered in light of (1) the nature and net cost of the accommodation needed; (2) the overall financial resources of the defendant and the number of persons employed by the defendant; and (3) the type of the Defendant's business, including the composition, structure, and function of the Defendant's work force.

Instruction 1.06[3][c]. *See also* 42 U.S.C.S. § 12111(10) (1998) (outlining factors to be considered in determining whether an accommodation would impose an undue hardship).

Instead, undue hardship must be based on an individualized assessment of current circumstances that show that a specific reasonable accommodation would cause significant difficulty or expense.[135]

The law may well require the employer to provide assistive technology to work in conjunction with or support a disabled employee's personal devices, or to reimburse them for the expense of assistive devices they already had acquired for use with their personal devices. These can be costly accommodations and consequently, an employer should be careful to address these issues when deploying a BYOD program. In particular, employers should:

- Train supervisors and employees on how to recognize an accommodation request with respect to a dual-use device.
- Recognize that reliance on a cost-prohibitive argument may not be enough to reject an employee's request for an accommodation.
- In the event an employee requests an accommodation (i.e., assistive technology or software), be prepared to engage in the interactive process with the employee (i.e., have a meaningful discussion with the employee about her needs and whether or how the company can meet those needs).

C. Wage & Hour Issues

1. Off the clock work

Allowing nonexempt employees to use their own mobile devices to conduct work-related business involves the risk that those employees will raise wage and hour claims for "off the clock" work. Even if a nonexempt employee uses his or her personal device voluntarily and without directive from the employer, the employee must be compensated for the time spent making work-related calls or reading and writing emails.

Both the federal Fair Labor Standards Act (FLSA) and state laws require that nonexempt employees be paid for all time worked, including overtime. This includes all time that employees are "suffered or permitted" to perform work.[136] Notably, it is not a defense that an employer did not instruct the employee to perform the extra work. Simply put, if the employee performed the work and there is any way for the employer to know that the work was performed, the employee must be paid, even if the work performed was not authorized in advance by the manager.[137] This situation commonly arises where nonexempt employees are receiving, reading, and/or responding to emails (or phone calls) during non-working hours. Because employees are likely to always have their personal device with them, this problem can be exacerbated if those personal devices now receive work-related emails and alerts during off-work hours.

An employer's initial response to avoiding overtime and off–the-clock liability may be to prohibit employees from accessing email or making/receiving work-related calls outside of working hours. In certain circumstances, this may be an employer's best option. However, this blanket prohibition may not be practical and may not outweigh the benefits

135 *See* 29 C.F.R. pt. 1630 app. §1630.15(d) (1996); *see also Stone v. City of Mount Vernon*, 118 F.3d 92 (2d Cir. 1997) (an employer who has not hired any persons with disabilities cannot claim undue hardship based on speculation that if it were to hire several people with disabilities it may not have sufficient staff to perform certain tasks). *See* 29 C.F.R § 1630.2(p)(2) (factors that an employer must consider in determining whether an accommodation poses an undue hardship).

136 29 U.S.C. §§ 203(g), 207(a); 29 C.F.R. § 785.11. ("Work not requested but suffered or permitted is work time").

137 29 C.F.R. § 785.12 ("If the employer knows or has reason to believe that the work is being performed, he must count the time as hours worked.")

to an employer in having a flexible workforce that is accessible remotely. Furthermore, the blanket prohibition may not be sufficient to avoid liability if it is not thoroughly communicated to employees and employees are not disciplined for accessing the employer's emails or making or taking work-related phone calls outside of working hours. Similarly, an employer's policy prohibiting unauthorized overtime, including overtime incurred through the use of mobile devices, is inadequate if it is not enforced by the employer.

If the off-the-clock email/phone call situation only arises on an incredibly rare basis (*e.g.*, twice a year) and the time taken to read and/or respond to an email or phone call is less than a couple of minutes, the employer may be able to take the position that the work is *de minimis* and need not be paid. However, the likelihood that off-the-clock work is *de minimis* is typically slight and this position is a risky one, especially where employees are using their personal devices to perform work. Rather, more commonly, employees frequently check their mobile devices throughout the day and evening, even on the weekend, and if they see a work email, they will read it and may very well respond to it. Even if it only took a minute or two at the most, the frequency with which the employee checks the device may eliminate the *de minimis* defense.[138] Also, the mobile device records will not only show that calls and emails were sent and received, but also how often this situation occurred, which is likely more common than rare. Further, it is not uncommon to see a manager responding back to an after-hours email from a nonexempt employee thanking him or her for responding so quickly, which not only reinforces that the nonexempt employee performed the work, but also that the manager clearly knew about it and should have made sure the employer paid the employee.[139]

Once an employer knows an employee is performing work outside of work hours, the question becomes, how can this work be tracked? As a general matter, employers should have a policy in place requiring employees to record all time worked, including time worked out of the office and outside regular office hours.[140] This policy can be expanded and clarified to expressly require employees to record time spent responding to emails and answering phone calls while out of the office. An employer may also institute a policy requiring prior written authorization to work remotely via mobile device. The policy could also address the timing for responding to after-hours emails and instruct employees that, unless they are directed to provide an immediate response, all emails should be responded to only during working hours. While employees' personal devices will obviously bleep, ring, buzz or otherwise alert them to every email or call received, even during non-working hours, this approach directs employees to ignore, and not spend time reading, or even opening emails from a manager or work colleague during non-working hours.

With the underlying policies in place, the employer must then communicate these policies to affected employees and consistently enforce the policies to ensure that all time spent accessing work-related emails or making/receiving work-related phone calls is tracked and recorded and that employees who do not comply with the policies are appropriately disciplined. Managers should also be trained to comply with the policy and recognize when they are

138 *See Lindow v. United States,* 738 F.2d 1057, 1063 (9th Cir. 1984) ("[I]n determining whether otherwise compensable time is de minimis, we will consider (1) the practical administrative difficulty of recording the additional time; (2) the aggregate amount of compensable time; and (3) the regularity of the additional work.").

139 In fact, because an employer's own data and device records will show when a nonexempt employee has performed work, the employer may have an obligation to regularly review such records in order to ensure employees are paid for such time worked.

140 Indeed, employers are required to keep accurate records of all time worked by nonexempt employees. *See* 29 C.F.R. § 516.2.

putting nonexempt employees in jeopardy of working outside of working hours (*e.g.,* sending an email to a nonexempt employee after hours). Managers could be instructed to begin emails sent to nonexempt employees during non-working hours with an instruction regarding whether the email is something that the employee needs to address immediately or the employee should wait to review and respond to the email during normally scheduled working hours.

One situation frequently overlooked is how to address employees who are on a leave of absence from work (*e.g.*, disability, maternity, etc.) and their ability to receive and respond to work-related calls and emails during a period when they are supposed to not be working. This situation arises not just with nonexempt employees, but also with exempt employees on an unpaid leave of absence.[141] One approach is to revise leave of absence policies to remind employees that they are not to be performing work during a leave of absence, and emphasize that this prohibition includes avoiding and not responding to all calls and emails received during this period. However, this type of approach rarely works when employees are already checking their device for personal calls and emails because completely disregarding, ignoring, and deleting all work-related communications can be incredibly challenging, especially if the employer is using the email system to communicate with the employee regarding his/her leave of absence status and eventual return-to-work. Obviously the most complete solution is to deactivate the employee's connection to the company's data and systems and/or reconfigure the system so calls and emails are redirected to another employee to address. If possible, this is the preferred approach because it minimizes the risk that employees will be performing work, for which they should be paid, during an unpaid leave of absence.[142]

Employers also need to carefully consider how they will handle the time employees spend procuring or repairing their dual-use devices. If, for example, the company decides not to directly support the employee devices and instead directs the employees to use third party service providers such as Apple's Genius Bar or Best Buy's Geek Squad, do they need to pay employees for the time they spend supporting the device? This problem may not be that significant for employers that only allow employees to use smartphones or tablets, but for companies that extend the program to cover laptops as well, the time spent troubleshooting PC repairs or configuration issues can be significant.

2. Expense reimbursement

An employee's use of his or her own mobile device also raises the question of whether the employer is required to reimburse the employee for the cost of the device, data plan, or monthly phone bill. Under federal law, the FLSA prevents employers from requiring an employee to pay for business expenses of the employer if doing so reduces the employee's earnings below the required minimum wage or overtime compensation.[143] Further, eleven states have express or implied statutory expense reimbursement requirements that may or could be interpreted to require reimbursement of an employee's use of his/her personal device for work-related purposes.[144]

141 The Federal Family and Medical Leave Act allows a salaried employee who satisfies the executive, administrative, or professional exemption under the FLSA to be paid on an hourly basis for work performed during a covered leave of absence. 29 C.F.R. § 825.206(a). However, for non-FMLA leaves of absence, such an employee's exempt status may be jeopardized if the employee is not paid in accordance with the salary basis requirements of the FLSA (e.g., full workweek salary typically must be paid for any workweek in which the employee performs work). *See* 29 C.F.R. § 541.600 *et seq.*

142 Employees' receipt of state disability benefits or short- or long-term disability insurance benefits may also be jeopardized if employees are performing work and receiving wage payments during a leave of absence that is supposed to be unpaid.

143 29 C.F.R. §§ 531.35; 531.36; 531.37.

144 California Labor Code section 2802 places a broad requirement on employers to reimburse all business expenses. Laws in Montana, North Dakota and

While a number of states require reimbursement, in particular, California law requires that employers reimburse employees for all "necessary expenditures or losses incurred... as a consequence of the discharge of his/her duties."[145] Unfortunately, there is not a great deal of guidance construing California's section 2802. However, it appears that whether or not expenses must be reimbursed will depend on whether or not the employees were required to incur the expense as a result of their employment.[146] If the use of the mobile device is entirely voluntary and solely for the employee's convenience, an employer may argue that the expenses need not be reimbursed. But, if employees are using their own devices to increase responsiveness and ensure positive performance evaluations, the voluntary use of the mobile device may become reasonable, and thus compensable as an expense.

Employers who are obligated to reimburse or who voluntarily decide to reimburse employees for the work-related usage of personal devices face the challenge of determining what amount to reimburse. Obviously the easiest method is for the employer to pay the full cost of the employee's device and cellular bills/data plan, but this approach results in overpayment to the employee. There are also tax implications to be considered. For reimbursement payments to be exempt from payroll and income taxes, the payments must be made pursuant to an "accountable plan."[147] To be deemed "accountable," an employer's reimbursement plan must satisfy three rules: (1) the expenses reimbursed under the plan must have a business connection, *i.e.*, they must be necessarily incurred as a result of the employee's work duties; (2) the employee must adequately account to the employer for these expenses within a reasonable period of time; and (3) the employee must return any excess reimbursement within a reasonable period of time.[148]

The more accurate reimbursement option is the actual expense method. This method involves reimbursement of the actual expense of using an employee's personal device for business purposes. Before smartphones, this was the preferred method because employees' cellphone bills showed every call made and it was possible to do a pro-rata allocation between business versus personal calls. Today this method is less viable where employees have flat fee or unlimited data plans, making it impossible to identify what portion of the device's usage was spent on business versus personal activities. Plus, in order for a reimbursement plan to be afforded tax-exempt status under an accountable plan, the information supplied by the employee must meet the Internal Revenue Service's very detailed recording and tracking requirements, which is not always possible with unlimited data and use programs.

South Dakota require reimbursement of all "necessary" expenditures incurred by an employee as a result of the discharge of the employee's duties, and would likely require reimbursement of an employee's personal device use. *See* Mont. Code Ann. § 39-2-701(1); N.D. Cent. Code § 34-02-01; S.D. Codified Laws § 60-2-1. There is no regulation or statute directly on point, but the Department of Labor in New Hampshire has taken the position that an employer need not reimburse an employee for personal mobile device use as long as there is a written agreement stating the employee will not be reimbursed for such expenses. *See* N.H. Rev. Stat. § 275:57 and telephonic opinion received on April 30, 2012. Laws in Alaska and Minnesota do not require reimbursement for equipment that employees may use for their own purposes outside of work. *See* 8 Alaska Admin Code § 15.160(a); Minn. Stat. § 177.24(4). Arkansas, Iowa, Kentucky and Michigan all have laws requiring reimbursement of any expense incurred by employees that would bring their compensation below minimum wage, which could result in a separate requirement to reimburse such expenses. *See* Code of Arkansas Rules and Regs., 010-14-107(A)(2); 875 Iowa Admin. Code 217.35(91D); Ky. Admin. Reg. 1:080(4); and MCLS § 408.477(1).

145 Cal. Lab. Code §2802.

146 *See Gattuso v. Harte-Hanks Shoppers, Inc.*, 42 Cal. 4th 554, 562 (2007) ("In calculating the reimbursement amount due under section 2802, the employer may consider not only the actual expenses that the employee incurred, but also whether each of those expenses was 'necessary,' which in turn depends on the reasonableness of the employee's choices.").

147 IRC §§ 62(a)(2); Treas. Reg. § 1.62-2(c)(4).

148 IRC §§ 62(a)(2)(a), (c); Treas. Reg. §§ 1.62-2(c)(1), (d)-(f).

California's Supreme Court has confirmed that employers in that state can satisfy their reimbursement obligations to employees by utilizing a lump sum payment method.[149] Under this method, the employer simply makes a fixed amount payment each pay period to cover an employee's business-related expenses. The payment can take the form of a periodic expense allowance or can be enhanced compensation, such as an increase in the employee's base salary, commission rate or hourly wage. Unfortunately, there is no set formula for an employer to determine what amount or percentage of an employee's monthly data plan would be considered business-related versus personal use.

Plus, while the lump sum reimbursement method may be simple to administer, it raises a concern regarding whether the amount being paid is sufficient to fully cover the employee's expenses. If an employer uses an enhanced compensation payment (*e.g.*, by increasing the employee's commission rate), the employer runs the risk that the employee earns lower than anticipated commissions, thereby not earning enough to fully compensate the employee for expenses incurred. In California, an employee must also be afforded the ability to challenge the sufficiency of a reimbursement payment and, if valid, the employer must pay the difference.[150]

Finally, the aspect that makes the lump-sum payment method so attractive–the lack of paperwork–may simultaneously make it the most risky from a tax perspective. Without an accounting of expenses submitted by employees, the lump-sum reimbursement method may fail to qualify as an accountable plan. As a result, all reimbursement payments are potentially subject to payroll and personal income taxes, thereby increasing both parties' tax burdens. Moreover, if the lump-sum payment exceeded the actual expenses, the employee would be obligated to return the excess or risk destroying the accountable status of the plan.

In sum, an employer should consider having a policy in place to track the use of dual-use devices for work purposes to ensure that employees are compensated to the extent the work performed on the devices is reasonable and necessary and reimbursement is required by state or federal law. If an employer wishes to have a work force that utilizes personal mobile devices for work purposes, the employer should evaluate the costs to be incurred by employees and federal and individual state wage and hour requirements, and determine whether to institute a policy to reimburse employees for expenses incurred related to the performance of work, including reimbursement for business-related phone calls, data plans, business applications and mobile devices with email capabilities. Reimbursement methods can provide for payment of actual expenses or a lump sum payment estimated to fully compensate employees, but determining the amount to be reimbursed and the tax treatment of these payments have inherent challenges.

D. Workplace Safety and Health (OSHA)

While an injury or illness caused by use of a device for purely personal use will seldom create employer liabilities, dual-use of a device can create work-related injuries and illnesses that are governed by the Occupational Safety and Administration (OSHA) and state workers' compensation law. Further, distracted driving while using a mobile device can result in injuries to employees and third parties that can result in significant liability.

149 *Gattuso v. Harte-Hanks Shoppers, Inc.*, 42 Cal. 4th 554 (2007).
150 *Id.* at 571.

1. **Repetitive stress–"Blackberry Thumb" and "Text Neck"**

The American Society of Hand Therapists (ASHT) has issued a warning regarding repetitive stress injuries to the thumb and many physicians agree. Similarly, other groups and physicians have warned that neck injuries can be caused by cradling a small cellphone between the head and shoulder or by continuously bending the neck straight down to read a small screen. When an employee begins using their own device for work-related purposes, the work relationship of any injury will be largely established and will be very difficult to separate from the effects of personal use of the device. These potential injuries will heighten the need for employers to provide training and guidance on ergonomic use of dual-use devices, including but not limited to appropriate body mechanics, total time spent using the device, and reporting any discomfort for appropriate review and responses.

2. **Brain injury from cellular signals**

Mobile devices emit a form of electromagnetic radiation called radio frequency (RF). During use, the body tissues next to where the phone is held absorb RF energy. Heating is the only known biological effect of RF energy. High doses of RF energy cause localized tissue heating, but RF exposure does not cause an increase in body temperature. A user's exposure to RF energy depends on several factors including: the model of the device; the amount of time the user spends on the device; whether the user is using a hands-free device; the amount of mobile traffic in the area at the time of use; and the distance to the nearest tower (the farther away the user is from a tower, the more RF energy it takes to get a signal). The amount of RF energy absorbed from the device is called the specific absorption rate (SAR). The Federal Communications Commission (FCC) regulates SAR levels, and device manufacturers must report the SAR level of their products to the FCC. The current SAR level limit is 1.6 watts per kilogram of body weight. To date there have been no successful legal claims regarding device phone radiation, but, as noted above, dual-use of a device may establish work relationship exposing employers to OSHA regulation or workers' compensation claims.

3. **Distracted driving and other activities**

Drivers can be distracted for many reasons, including mobile device use. According to the National Highway Safety Council, nearly 5,500 people died (16% of all fatalities) and 500,000 were injured in crashes in 2009 involving a distracted driver. Statistically, a texting driver is 23 times more likely to be involved in a crash. Further, a study by *Car and Driver* found it takes a texting driver twice as long to react than one who is legally intoxicated.

Based on these statistics, the Occupational Safety and Health Administration (OSHA) started a Distracted Driving Initiative. While the initiative covers all reasons for distracted driving, OSHA's initial emphasis is on the dangers of texting while driving. In addition to encouraging employers to have a policy prohibiting employees from texting and talking on cellphones while driving, OSHA states it will investigate and issue citations under the General Duty Clause if it receives a complaint that a company requires its employees to text while driving or "organizes work so that texting is a practical necessity." The General Duty Clause is a catch-all for OSHA, and simply obligates employers to create and maintain a safe and healthful workplace. Monetary penalties for General Duty and other OSHA violations are limited by statute and are based on the severity of the incident and the employer's past safety record, among other factors. However, of greater financial concern is the possibility that an employer will be liable for damages to persons injured

in an accident caused by a worker using a cellphone while driving on company business. There have been several jury verdicts and settlements in the $15-25 million range in cases involving drivers who were allegedly distracted by using their cellphones as part of their work.

Other than OSHA's intended enforcement of the initiative through its General Duty Clause and a DOT guidance banning commercial truck drivers from texting, the federal government has not enacted any laws prohibiting talking or texting while driving, although Transportation Secretary Ray LaHood has identified distracted driving as a "national epidemic" and called upon Congress to enact a law for a federal ban applicable to any type of vehicle on any road in the country. Several states, however, have passed laws of this nature: 30 states plus the District of Columbia and Guam prohibit all drivers from texting while driving, and eight states and the Virgin Islands prohibit all drivers from using hand-held cellphones. Other states only prohibit school bus drivers from using a cellphone while driving (*e.g.*, Arizona) or teens from talking and/or texting (*e.g.*, Indiana). No states have banned all cellphone use while driving, despite research showing no difference in accident rate when a driver is holding the cellphone versus using a hands-free device.

According to the DOT, over 2,000 U.S. companies already have adopted distracted driving policies covering over 12 million workers. Implementing and enforcing an effective mobile device use policy not only protects employees and the public from the dangers of distracted driving, it also can reduce OSHA citations and protect companies from being responsible for paying high amounts in damages for accidents caused by device use while driving.

E. Deploying BYOD in a Unionized Workforce

All employers, irrespective of whether they are unionized, should be aware of certain concerns related to device policies and monitoring employee use, as there is the potential for liability under the National Labor Relations Act (NLRA).

1. Consult applicable collective bargaining agreements

If a company is considering implementing a BYOD program and has a unionized workforce, it should consult the terms of the collective bargaining agreement covering the employees to determine if there are any applicable restrictions. For a unionized workforce, merely implementing mobile devices of any type into the workforce may be subject to bargaining, depending on the terms of the collective bargaining agreement. The two-part test used to determine whether the implementation is a mandatory subject of bargaining is whether it: (1) is "plainly germane to the 'working environment'"; and (2) does not amount to those "managerial decisions, which lie at the core of entrepreneurial control."

2. Implementing a policy is a mandatory subject of bargaining

Once an employer decides to use mobile devices, the implementation of a policy or plan to govern employees' use of these devices is a mandatory subject of bargaining according to the National Labor Relations Board (NLRB). An employer needs to decide whether its policy will require employees to follow all other employer policies, including the non-solicitation policy and any restrictions that the employer imposes on social media activity. Importantly, the NLRB has issued decisions recently affecting these and other policies, and the policies in question should be discussed with counsel for potential concerns. A policy for a unionized workforce need not be identical to a policy for the employer's non-unionized workforce and may provide for different restrictions or rights.

3. Monitoring the device is permissible if consistent in frequency and scope

When crafting the policies that will apply to dual-use devices, employers must determine whether and to what extent they will monitor the use of the devices. Monitoring may take the form of reviewing applications employees install on their dual-use devices to prevent the installation of insecure apps or monitoring the websites employees visit to ensure employees are adhering to other company policies. If an employer decides to monitor employees' use, non-unionized and unionized employers alike need to be careful since the NLRB considers surveillance of employees unlawful when a company's monitoring impinges on an employee's right to engage in organizing activities or otherwise exercise his or her Section 7 rights. In general, the use of *overt* surveillance or monitoring for legitimate business reasons such as theft or violence is permissible under the NLRA, irrespective of union presence. This is true even in the middle of an organizing campaign. However, employers need to be careful of the limitations on their ability to monitor employees in circumstances that involve union campaigning or protected, concerted activity.

Specifically, employers cannot use the monitoring to identify union activity nor can they use the monitoring in a manner that would tend to interfere with, restrain, or coerce employees in the exercise of union activity. If employers stumble across employees engaged in union activity, the employer will need to be able to prove it was engaged in a legitimate practice (for instance, monitoring for safety or theft reasons and the employer did not change the focus or frequency of the monitoring). In addition, employers cannot give the impression of monitoring for union activities, such as suggesting the monitoring of employees' email or text communications to a union business agent, even when no monitoring is actually occurring. The NLRB has found that the surveillance of workers, or the impression that workers are being watched, can constitute unlawful interference with Section 7 rights because it may give workers the sense that management is peering over their shoulders and thus stifle protected activity.

4. Electronic devices affecting the terms and conditions of employment

When an employer is given the discretion on how to implement state or federally mandated regulations, the NLRB takes the position that it is required to bargain over the implementation and effects of any changes. For example, if a company wanted to install an App on mobile devices to change the method for reporting hours of service under the Department of Transportation regulations from a paper log to an automated log, the company would need to bargain with the union over the implementation and the effects of such change. There are conflicting decisions in this area, however, and other decisions have stated that when the technology merely changes the way an employee reports his or her location, such as moving from a manual two-way radio to a Global Positioning System (GPS), such change is not a mandatory subject of bargaining. What is clear is that when the company intends to use data from dual-use devices when issuing discipline, potentially affecting an employee's continued employment, such impact is a mandatory subject of bargaining.

5. Union's right to view or obtain a copy of the data gathered

Companies operating in a unionized environment must also remember the union has the right (usually in the context of an investigation or a grievance) to obtain information from the company concerning the data or images captured by any existing cellphone, cameras or electronic devices unilaterally installed by the employer. Before an employer elects

to use any features of mobile devices or their applications to track employees' locations or the applications installed on their devices, for example, the company should consider the potential obligation to provide this data to the union. Moreover, the company may demand to bargain with the union over appropriate confidentiality terms relating to the release of such information.

F. International Legal Challenges

Several cross-border challenges exist for companies with employees who work outside the United States or who travel internationally.

1. Border security searches

Employees who travel internationally run the risk of a search by border control and security staff of the foreign country they visit and upon their return to the United States. Unlike other searches by an agent of the U.S. government, a search at the border does not require a suspicion of criminal activity.[151] The Department of Homeland Security (DHS) in 2009 issued specific directives that address the search and detention of international travelers' electronic devices. To this end, the Directive[152] issued by the U.S. Customs and Border Protection (CBP), covers a wide array of electronic equipment and provides "guidance and standard operating procedure for searching, reviewing, retaining, and sharing information contained in computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices." Similarly, the U.S. Immigration and Customs Enforcement (ICE) issued a Directive[153] to its officers regarding their "border search authority to search, detain, seize, retain and share information contained in electronic devices possessed by individuals at the border."[154]

The traveler's consent is *not* required for the search.[155] Further, asserting that the information is protected against disclosure under the attorney-client privilege will not necessarily exempt the data from the search.[156] The Directives guide the officers to consult with the agency's legal counsel or the local attorney's office before proceeding with the search.[157] Business's confidential information and other sensitive information (such as medical records) will be treated with "special care," but again is not exempted from review and analysis.[158] Finally, the agent may detain the device for days to complete a "thorough border search," which could cause major inconvenience.[159]

151 *See* Bret E. Rasner, *International Travelers Beware: No Reasonable Suspicion Needed to Search your Electronic Storage Devices at the Border*, 3 Phoenix L. Rev. 699 (2010).

152 CBP Directive No. 3340-049, Aug. 20, 2009.

153 ICE Directive No. 7-6.1, Aug. 19, 2009.

154 *Id.*, Section 1.1

155 *Id.*, Section 8.1(3).

156 CBP Directive Section 5.1.1 and ICE Directive Section 8.6(2)(b).

157 *Id.*

158 CBP Directive Section 5.2.2 and ICE Directive Section 8.6(2)(a) and (c).

159 Under the CBP Directive, the detention can be up to five days. Section 5.3.1. The ICE Directive, however, states that searches "generally [should] be completed within 30 calendar days."

2. Risk of commercial espionage activity

According to recent press reports[160] a number of foreign governments and some companies in certain foreign countries have improved their technical ability to remotely access electronic devices used in their territories to harvest data. Due to the increased risk of such unauthorized access to and downloading of confidential business data, companies have taken precautionary measures such as issuing their employees who travel international with loaner devices that have been scrubbed of all company confidential information.

3. Stricter control of working hours

The wage-hour laws in foreign countries differ in two major respects from the Fair Labor Standards Act and similar U.S. state laws. First, the class of employees who are exempt is very small, and frequently limited only to a handful of top executives. Second, the laws set maximum weekly or monthly working hours (which includes overtime hours). As a result, employers must restrict working hours or face enforcement action and penalties. To effectively control actual working hours of employees, companies in Europe, such as Volkswagen in Germany, are shutting down their e-mail servers after hours so employees cannot work. Only very senior executives are exempt from this preventive measure. In the instance of Volkswagen, the e-mail servers stop routing e-mails 30 minutes after the end of employees' shifts, and resume 30 minutes prior to the start of their shift the next day.[161]

4. Privacy challenges outside the United States

The privacy laws protecting personal information of employees in other countries are quite different than those in the United States. A discussion of the differences is beyond the scope of this Report, but U.S. companies with employees outside the U.S. should carefully evaluate their BYOD policies and their planned use of software to manage the devices to ensure they comply with local laws.

While an in-depth analysis of privacy issues related to BYOD in the international context is beyond the scope of this Report, the International Guide to Employment and Labor Law should be consulted as it covers privacy and related employment law issues in 54 countries plus a chapter on the European Union.

160 *See, e.g., Traveling Light in a Time of Digital Thievery*, N.Y. Times, Feb. 1, 2012.

161 *See Volkswagen turns off Blackberry e-mail after work hours*, BBC News, Dec. 23, 2011, *available at* http://www.bbc.com/news/technology-16314901.

V. RECOMMENDATIONS

Over the next year to no more than three years, virtually every company will need to address the issues raised by this Report. The significant growth of mobile devices and their use by employees to conduct business–with or without the company's support–combined with the continued blurring of the line between personal and work lives will force employers to respond. Companies will make different decisions depending on the company's employee mix, the sensitivity of the data they handle, the mobility of their workforce, the company's risk tolerance, and other factors. For some, a BYOD program will be the best response. For other companies, a more appropriate approach may be to offer employees a greater choice of mobile devices and retain ownership of the device that stores company data. However, for this approach to gain traction with employees frustrated by carrying two devices, companies may need to also relax traditional restrictions on the use of company technology for personal use.

For those companies that choose to follow the BYOD approach, the following recommendations will help navigate the complicated employment law issues.

A. Implement New Policies

Due to the wide variety of issues a BYOD program creates, it is challenging to provide a single sample policy for an employer to adopt. This difficulty is made even more challenging with an attempt to adopt one global BYOD policy. Rather, the policy and technology decisions the company makes will likely require subtle modifications to many existing policies, including:

- Harassment, Discrimination, and Equal Employment Opportunities
- Workplace Safety
- Time Recording and Overtime
- Acceptable Use of Technology
- Compliance and Ethics
- Data Privacy and Security
- Records Management
- Litigation Holds
- Confidentiality and Trade Secret Protection

Below, we have outlined basic recommendations for new or revised policies that touch on all of these areas.

1. Decide which employees should be permitted to participate in a BYOD program

As noted in several sections above, dual-use devices may not be appropriate for all employees within a company. Employees in some positions pose greater challenges, and perhaps should not be allowed to use dual-use devices, such as:

- Senior executives whose data is more likely to be relevant in litigation.
- Employees in research and development roles who are likely to handle trade secret information.

- Sales staff who may have a hold on the goodwill of customers and who, because they are using a personal device, will continue to use their same telephone number when they take their device with them when they leave.
- Nonexempt staff who could claim the dual-use device caused them to work "off the clock".
- Contractors and other contingent workers who may be simultaneously performing work with their personal devices for other customers.

2. Address off-the-clock work

If nonexempt employees will be permitted to use dual-use devices, address the use of dual-use devices outside work hours as well as the need to properly record time. If the devices used by employees allow for different rings or alerts for incoming work and personal emails or messages, consider requiring employees to use them to distinguish work and personal alerts. This may help limit claims by employees for overtime pay for checking their devices every time a work-related message arrives during off hours.

3. Check collective bargaining agreements

Companies with unionized work forces should also review their collective bargaining agreements to determine whether their policies regarding handheld devices, whether BYOD or not, are covered. If so, a best practice is to bargain, at least to impasse, the implementation of the policies and issues regarding how violations of those policies–as well as the use of information collected from the devices–will be used for disciplinary purposes. Having policies and procedures in place to ensure any monitoring is routinely reviewed and followed by appropriate investigation and disciplinary action when necessary will help reduce the risk of liability from a labor management standpoint.

4. Reduce expectations of privacy

Be clear with employees regarding the issue of their privacy when using dual-use devices and the company's possible need to access their device for record retention or litigation holds or investigations. If preservation for litigation is necessary, companies will likely need to copy the entire device and will not be able to differentiate between personal data and company data at the time of collection.

5. Require employee consent

Before allowing employees to use dual-use devices to perform work, companies should obtain their written consent to:

- Monitor the device, including the data they store on it and transmit with it.
- Remotely wipe the device, including any personal information they have stored on the device.
- Install security software to manage the device and secure the data stored on it.
- Copy their data to meet litigation hold demands and record retention obligations.

6. Access is a privilege

Company policies should make clear that the ability to use a dual-use device is a privilege, not a right, and that access can be terminated at any time.

7. All other policies apply

Companies should remind employees that all other company policies apply when they use their dual-use device during work hours or on work premises, including policies against discrimination, harassment, acceptable use of technology, etc. Companies should also consider modifying existing policies to ensure they cover new challenges, such as:

- Harassment by coworkers for off-duty conduct that creates a hostile work environment.
- Responding to accommodation requests from employees related to dual-use devices.

8. Provide dual-use devices upon demand, preserve data, and delete backups

Because dual-use devices will contain company data, it is likely that at some point the need will arise to retrieve data from the device to comply with litigation holds, internal or regulatory investigations, or record retention obligations. Employees will need to provide access to the device for this to occur. Employees should be instructed to preserve this data, and not destroy or alter it, until it can be copied from the device. In addition, employees must understand the need to remove company data from any backup copies or synchronized versions of their devices that may exist on the employees' other personal computer devices, storage systems, or cloud-based storage services or applications.

9. Follow good security practices

Due to the inherently mobile nature of dual-use devices, they are frequently lost or stolen. Employers should consider at least the following security options:

- Regularly remind employees to use strong passcodes to protect their device.
- Require that employees not disable or alter the security settings on their devices.
- Prohibit employees from upgrading the operating system on their devices until the company has had an opportunity to ensure that Mobile Device Management software will continue to protect the device.
- Use the Mobile Device Management software to force strong passwords, or at least prohibit simple passwords.
- Remind employees they must take care to physically secure their device against theft, loss, or unauthorized use.

10. Immediately report lost/stolen devices

Most Mobile Device Management software gives employers the ability to remotely delete all the data stored on a device, which is commonly referred to as "wiping" a device. However, this command cannot be sent successfully unless the device has battery power and is active on the cellular network or Internet. If an employee does not report the loss or theft of a device immediately, the company may not be able to send the wipe command to the device. Therefore, employees should be required to immediately report any lost or stolen devices.

11. Compliance with configuration instructions

The operating system for the device, as well as the Mobile Device Management software or other security software, will almost certainly need to be configured or updated from time to time. This will likely require employees to take

manual steps to assist in the process. Therefore companies should require employees to assist with this process and comply with all instructions regarding the configuration of the device.

12. No friends and family

Unless the company has used security software (described below) that creates a separate, password-protected "Sandbox" to segregate company data from personal data, companies should prohibit employees with dual-use devices from sharing those devices with friends and family. This may be very difficult to enforce, but can be critical to the protection of company data.

13. Limit use of cloud-based storage for company data

Employees using dual-use devices should be instructed not to use any cloud-based storage or services to store company data without approval of the company. This will ensure sensitive personal or financial data, and company trade secrets are not stored with vendors that do not have appropriate security controls in place and a contract that binds them to protect this data.

If remote backup or sharing of files is important for business purposes, companies should consider following IBM's lead and develop their own "fit for business" plans. By building their own Apps to provide necessary functionality, they can meet employees' needs but mitigate the risks to company data. If this is not feasible, companies can explore developing master agreements with cloud vendors that will apply to employees' use of the service.

14. Help desk support

Companies must decide whether they will provide help desk support for employees' dual-use devices. If not, they should consider what steps employees should take before they seek support from third-party vendors to prevent company data from being accessed during the support process. For example, companies may wish to remotely delete data from employees' devices before they seek support. Companies should also carefully evaluate whether they are required to compensate nonexempt employees for the time they may spend fixing and maintaining their dual-use devices.

15. Mobile device safety

Regardless whether any given state has laws regarding the use of cellphones or texting while driving, companies should adopt a policy outlining the rules for employee use of cellphones, mobile devices, and other distracting technology while driving on company business, including:

- A statement that the company does not tolerate texting or talking on a hand-held device while operating a company vehicle or while operating a personal vehicle on company business, including answering or making phone calls, engaging in phone conversations, viewing the Internet, and reading or responding to e-mails and text messages.
- Instructions to employees on what they should do, such as pulling over to a safe place when a call is made or received or an email or text message needs to be read or sent; changing voice mail greetings to indicate they are not available to answer calls or return messages while driving; and informing customers about the policy to explain why they sometimes may not be able to answer or return calls, emails, or text messages immediately.

An effective policy not only supports an isolated employee misconduct defense when an employee engages in distracted driving under OSHA, it also may limit or even eliminate a company's liability for damages for accidents caused by employees talking on cellphones or texting while driving. An effective policy also can be used to prove the employer took reasonable measures to prevent distracted driving accidents, thereby adhering to the proper standard of care.

16. Consequences for failure to comply

Remind employees that a violation of policies applying to dual-use devices, just like all other company policies, will lead to disciplinary action, up to and including termination.

B. Develop Employee Agreements

To be effective, many of the policies listed above must apply to employees after they leave the company. To ensure they will still apply after the employee leaves, companies should consider addressing these issues in an agreement with the employee and require employees to execute these agreements as a condition of being allowed to use dual-use devices.[162] If the company already has confidentiality, non-compete, or non-solicitation agreements that address post-employment activities, these provisions could be added to those agreements.

1. Arbitrability

Inevitably, disputes will arise between employers and employees concerning the use (or misuse) of electronic devices. These could include disputes over ownership, privacy, cost, repair, breaches in security, post-employment retention of data, misappropriation of trade secrets, harassment, disability accommodations, and more, including novel issues that cannot even be contemplated at this time. Arbitration may be one avenue for resolving these disputes and may have several advantages over court litigation, including lower costs, greater efficiency, increased privacy and having a neutral expert fact finder (usually a veteran attorney or retired judge) resolve the matter.

Almost certainly, disputes related to dual-use devices would be arbitrable. The United States Supreme Court recently held that unless Congress specifically excludes a particular dispute from arbitration, the Federal Arbitration Act (FAA)[163] requires that courts enforce agreements to arbitrate the dispute.[164] Therefore, in the absence of a federal statute banning arbitration of disputes relating to personal devices, companies covered by the FAA (for the most part any company engaged in interstate commerce is covered, although certain classifications of workers engaged in interstate transportation are not[165]) should be able to require employees to submit disputes related to dual-use devices to binding arbitration.

The arbitration agreement can be drafted to broadly cover any and all disputes arising out of or relating to the employment or can be limited to disputes arising out of or relating to the use of the dual-use devices.[166] In the latter case,

162 However, companies with unionized employees must use care when using arbitration clauses, because a Company cannot contract directly with employees over terms and conditions of employment that are a mandatory subject of bargaining. See note 1015, *supra*.

163 9 U.S.C. §§ 1 – 16.

164 *Compucredit Corp. v. Greenwood*, 2012 U.S. Lexis 575 (Jan. 10, 2012).

165 9 U.S.C. §§ 1, 2.

166 "[P]arties may agree to limit the issues subject to arbitration." *AT&T Mobility L.L.C. v. Concepcion*, 131 S.Ct. 1740, 1748 (2011).

in exchange for being able to use their preferred personal device, employer contribution to or funding of the purchase of the device or the monthly data plans, the employee would be required to agree to arbitrate device-related disputes. In the former situation, an agreement covering all disputes arising out of relating to the employment relationship likely would be construed to include disputes relating to the device.[167] For employers who already have implemented a broad form arbitration agreement, disputes relating to dual-use devices likely already are covered. Therefore, if employers do not want to have disputes related to dual-use devices included within the scope of their agreements to arbitrate, it will be necessary to modify the agreements to expressly include a carve-out for such disputes, making them non-arbitrable.

Care must be taken in drafting or creating exceptions to any ADR agreement. For example, if an employer carved out of its arbitration program all disputes relating to the use of a dual-use devices, could an employee covered by that agreement who claims to have been shown sexually explicit photographs that a coworker maintains on his device claim that her sexual harassment claim is no longer arbitrable because it arises from her coemployee's "use" of his dual-use device? Here, as in many areas of labor and employment law, perhaps the issue may not so much be a "be careful what you wish for" problem, but rather one that arises from the concomitant "law of unintended consequences."

C. Implement Technical Controls

Many of the risks discussed above can be mitigated by the use of software that allows a company to control dual-use devices. The specific controls differ from depending on the device and the mobile platform it uses.[168]

1. Mobile Device Management software

Most mobile devices can be managed using Mobile Device Management (MDM) options built into the operating system for the device. These MDM features allow companies to remotely manage and configure many aspects of dual-use devices. Some of the more common security controls these tools allow a company to implement include:

- Require encryption of all data stored on the device
- Require strong passwords for access
- Force the wipe of the device after 10 unsuccessful password attempts
- Lock the device after a period of inactivity to prevent unauthorized use if the device is inadvertently left available or is lost or stolen
- Prohibit "jailbroken" devices[169]
- Use the remote wipe features to delete all data on the device
- Use remote location features (e.g. the iOS "Find My iPhone" feature)

167 "[A]ny doubts concerning the scope of arbitrable issues should be resolved in favor of arbitration...." *Moses H. Cone Mem'l Hosp. v. Mercury Const. Corp.*, 460 U.S. 1, 24-25 (1983).

168 For example, an Apple publication entitled Deploying iPhone and iPad Mobile Device Management describes the many options available for configuring Apples iOS devices, including iPhones and iPads is available at http://images.apple.com/iphone/business/docs/iOS_MDM.pdf.

169 The term "jailbreak" refers to the process of bypassing features or protections built into the Operating System of the device. For example, some users "jailbreak" Apple iPhones to allow them to be used with other cellular carriers or to install applications not approved by Apple. The process of jailbreaking a device can introduce security vulnerabilities.

- Prevent the installation of an unapproved applications or blacklisting others
- Forcing the encryption of device backups

Companies should carefully review the features provided by the MDM software and decide which should be used and how they should be configured to best meet the company's goals and culture. Afterward, steps should be taken to validate that the software was successfully deployed and that all the desired settings were implemented.

This type of software is readily available on almost every type of mobile device platform available today. Given the level of risk mitigation MDM tools offer, employers should consider leveraging these controls almost as a matter of course. However, as noted below, the adoption of these controls must be accompanied by appropriate policies and training.

2. Consider creating a separate corporate "Sandbox"

In addition to the basic MDM options, some companies now offer software that creates a virtual container or "Sandbox" for the storage of company information and the applications employees can use to work with that information. This Sandbox approach can help segregate work from personal data. If a "wipe" command needs to be sent to the device, this type of software can limit the deletion to the data in the corporate "sandbox."

While this software can provide additional protections and capabilities, companies should be careful not to assume that it entirely addresses all risks. Companies will still need to rely upon policies, agreements, or training of their employees to ensure they do not create, store, or transmit company data using applications located *outside* the corporate Sandbox. The Sandbox approach also provides no protection for the company data that employees store with cloud-based services.

3. Limit the BYOD program to platforms the company can support

Before allowing employees to choose particular devices as part of a BYOD program, companies should carefully evaluate the platforms and operating systems and ensure they can effectively manage them using the selected MDM software. Vendors update Apps, operating systems, and devices on a regular basis. The combination of these changes can be challenging to manage given the constant development cycle. As a result, companies may find it advisable to limit the types of devices and platforms employees can use to allow the company to ensure adequate management of the devices.

4. Use enterprise Apps or virtualization technologies to limit the data stored on dual-use devices

Companies can also limit the amount of corporate data that is stored on employees' dual-use devices by choosing how to allow access to company data. Some companies allow employees to use their personal devices as a method to access data stored on the company network, while prohibiting them from downloading the data to their devices. As noted earlier in this Report, Citrix offers software that allows employees to securely access a version of their company computer and the network using their personal devices. By eliminating, or at least limiting, the company data stored on the device, many of the data-related concerns can be addressed or at least mitigated.

Other companies are creating company-sponsored Apps that allow employees to interact with corporate systems and obtain information they need to do their job while controlling how much data is actually stored on their personal devices.

D. Implement New or Revised Operating Procedures

In addition to new or revised policies, companies must also consider whether they need new operating procedures to deal with the challenges posed by dual-use devices. The sections below describe some of the operating procedures a company should include in its initial review, and this list should be supplemented by controls necessitated by a company's particular policy choices and corporate culture.

1. Plan for lost or stolen devices

Employers should develop and test internal processes for employees to follow when their devices are lost or stolen. If the company does not already have an established reporting process, it should consider identifying a department or group within the company–typically the IT support or help desk function–to be the central place to which employees can report that their devices have been lost or stolen.

2. Develop a remote wipe process

The group that receives reports of lost or stolen devices must understand how to use the MDM software to delete data from the device. These staff also need to be sensitive to the pitfalls of executing a remote wipe in situations where employees have not consented to this action. In any event, a remote wipe command usually must be sent quickly due to the relatively short battery life of many mobile devices. Once the device has lost power, or is no longer on a network, the device can no longer receive the wipe command.

3. Remind PC users to implement antivirus protection at home

Employers should remind employees to install up-to-date antivirus software on their home PCs or other devices to which they synchronize their dual-use device (if such sychronization is permitted). Many mobile operating platforms include this functionality, and when the device is synchronized the data can be backed up to the employee's home PC. If this data is not encrypted, it could be subject to unauthorized access if the employee has malware on their home computer.

4. Revise exit interview processes

Because employees will now have corporate data stored on their own personal devices, the company's exit interview process will need to be reevaluated to ensure that corporate data is removed from the device, as well as from any backups or cloud-based storage used by the employee.

In situations where an employee may have stored on her device company trade secret information, data subject to a litigation hold, or data that must be protected due to various privacy regulations, the company should carefully review the following as a part of the exit interview process.

- What devices the employee used, had access to, and submitted on any expense reports.
- What information may be stored on the employee's dual-use devices.

- What efforts should be used to preserve data stored on the employee's dual-use devices before the device is wiped and whether the company needs to retain an outside forensic consulting firm to help preserve and collect this evidence. All too often a company's well-intentioned IT staff can irreparably damage electronic evidence.
- Disable the employee's ability to connect all mobile devices to the company's systems.

5. Revise litigation hold policies and procedures

Companies should revise their litigation hold policies and procedures to ensure that dual-use devices are included in the scope of litigation holds. Moreover, the company should ensure that its staff or vendors that perform collections of data for litigation are trained and have the tools necessary to collect data from the wide variety of devices used by employees.

Companies should also educate managers, IT staff, and legal counsel about the risks of accessing employee data stored in personal e-mail accounts and other online services and develop a policy for addressing such access.

Employers should also develop clear policies and procedures for IT staff to follow when collecting and reviewing data from employees' dual-use devices to protect against access to information that may create additional risk for the employer, including evidence of disabilities, genetic information, personal or attorney-client privileged information of the employee, as well as usernames or passwords that may provide access to personal e-mail accounts or cloud-based storage that may be protected by federal or state laws.

6. Continuously update procedures and policies

Because the operating systems and applications available to mobile device users change rapidly, companies should regularly reevaluate their policies, procedures, and agreements to identify new risks that need to be addressed.

7. Evaluate insurance coverage

Companies should also evaluate their insurance policies to determine whether additional "cyber-risk" policies may provide additional protection or mitigate the data-related risks described in this paper. Companies should also consider checking with their insurance companies or brokers to verify that incidents arising from employees' use of their own personal devices are covered by the company's insurance policies.

8. Revise contingent worker contracts

Companies that use contingent workers should review their contracts and add provisions that prohibit or strictly regulate the use of personal devices by contractors and contingent workers and require that they adhere to the company's other information security policies and procedures.

9. Evaluate reimbursement plans

Companies should consider whether the reimbursement policies they have adopted comply with applicable laws regarding employee compensation. Whether and how much reimbursement for device costs or monthly plans is required will depend on a variety of factors, including what employees are allowed to participate in a BYOD program, the extent of use of dual-use devices, whether employees can use the company's IT help desk service, etc.

E. Training

Depending upon the specific policies each company develops, the content of training and awareness activities related to these issues will differ. However, for these risks to be adequately mitigated, companies should review their current training and awareness programs and update them to cover these topics.

F. Risk Management Approach

Managing the risks of a BYOD policy can be challenging, as the scope of the above Recommendations make clear. Employers that look at risk and opportunity as two sides of the same coin are more apt to seize competitive opportunities without taking on unknown or unmitigated risk. Some of the opportunities–reducing costs, employee convenience, more direct access to customers–are appealing, but beneath the surface are a number risks that employers should assess before deciding to allow dual-use devices to be used as a part of standard business processes.

The "LITTLER" Risk Management Framework provides companies with a structured process for assessing risk and developing policies and procedures to effectively manage them. This Framework has several steps.

1. Lead

The first step in the process is to assign a person or team to own and manage specific key risk areas. As described above, dual-use devices create a number of emerging risks, and employers should be preparing now to assign risk responsibility to an executive with a multi-faceted experience or to a team that will possess, collectively, a broad understanding of the business, how these devices will be used, and how to effectively mitigate risk going forward.

2. Inspect

Once the employer assigns ownership of the risk, the next step is to thoroughly inspect the risk area. Are there gaps in existing internal controls? How do the potential financial, reputational, criminal, and strategic risks described in this Littler Report apply to the company? The knowledge and data collected in the inspection phase will be instrumental in designing and implementing risk mitigation initiatives.

3. Teach

Risk management must also include a teaching component. Merely writing an effective policy will not reduce risk unless the right employees are taught the policies and procedures they must comply with to manage the risks.

4. Train

While the teaching step is the "what" of risk management, training is the "how." Employers must train employees to know how to react in given situations. Therefore, an effective risk management program must include real-life, fact-based scenarios that enable employees to react effectively if an event occurs.

5. Launch

Employers must decide how much risk they are willing to take. The most effective approach to seizing a lucrative opportunity is to reduce or mitigate a competing risk to the point that it fits within the employer's risk appetitive. Employers must launch mitigation programs and initiatives that support the ultimate business strategy.

6. **Examine**

Risks are like living organisms. They shrink and grow, multiply and divide. Risk management is not a stagnant actively. Employers must continually examine their risk inventory and the relative rankings of those on the inventory as well as new and emerging risk areas. As mobile technology continues its rapid development pace, companies must continually reassess the risks posed by new features and functionality (*e.g.* speech recognition, geolocation, social media, collaboration and project management tools, video conferencing capabilities, etc.) and update their approach accordingly.

7. **Report**

Finally, the risk management function must report to stakeholders the key information that will allow the employer to continually improve its risk management function and the overall business.

In the final analysis, the risks described in this Littler Report cannot be addressed in isolation. Mitigation of these risks requires a cross-functional approach that includes:

- Careful review and application of the available Mobile Device Management options available in the devices, platforms, and operating systems to control the devices and the data stored on them.
- New or revised policies to address the risks in a way that is in line with each company's values, risk tolerance, and corporate culture.
- New or revised operating procedures that breathe life into the polices selected by the company.
- Education and training of all affected employees.
- Regular re-evaluation of the risks as vendors introduce new features and functionality that affect or create new risks.

VI. CONCLUSION

When companies as traditional and respected as IBM and Kraft deploy BYOD programs, it is clear the BYOD Movement is not a short-lived trend, and that more companies are likely to adopt dual-use device programs–despite the risks. Over the next one to three years virtually every company will be forced to address these issues as more employees purchase mobile devices with new functionality and always-on connections to the Internet. These employees will increasingly resist carrying a company device in one pocket and a personal device in the other. The ability to perform work from almost anywhere will also continue to minimize the distinction between work life and personal life for many employees.

Technology has advanced to the state that our personal and business lives overlap, yet our laws and regulations are years behind. This demands that employers try to adapt and adjust traditional mandates and requirements to minimize risk and maximize compliance while the BYOD Movement accelerates.

Whether an organization is prepared to adopt a comprehensive BYOD program or not, every employer will need to address the question of how to react to the inevitable and growing use of personal devices in performing work. Those employers who decide to adopt a BYOD program to allow and regulate dual-use devices should review the risks and recommendations described in this Report and then develop policies, procedures, and technical controls to address them. Cookie cutter approaches will likely not work. Rather, an employer's approach will work best if it is tailored to the company's specific business model, regulatory environment, and corporate culture. Then those organizations electing to not allow dual-use devices will also need to examine their compliance, business and legal risks as it becomes increasingly easy and commonplace to apply personal devices to business tasks. The acceleration of the BYOD Movement may be slowed, but stopping it is comparable to prohibiting dating between coworkers. It can be done, but it is increasingly in conflict with the way the smartphone and tablet generations approach life both in and outside the "workplace."

Unfortunately, setting up a BYOD program is not likely to be a one-time event for organizations. This is a dynamic area, and new features and applications invented for mobile devices are potential challenges for the employer. This constant state of change will require continued diligence and a re-examination of the benefits, risks and responsive choices by employers through their management, corporate counsel, HR professionals and IT departments. Littler commits to continue bringing employers worldwide employment and labor law solutions needed today to be prepared for the workplace of tomorrow.

Endnotes

a. D.C. District Court - *DL v. District of Columbia*, 251 F.R.D. 38, 46 (D.D.C. 2008) ("With regards to the term 'control,' it has been well established that the test for control is not defined as mere possession, but as the legal right to obtain such documents on demand."); First Circuit - *Haseotes v. Abacab Int'l Computers, Inc.*, 120 F.R.D. 12, 15 (D. Mass. 1988) ("legal ownership is not the determining factor... Under [Rule 34], a party has 'control' over a document if that party has a legal right to obtain those documents."); Third Circuit - *Mercy Catholic Med. Ctr. v. Thompson*, 380 F.3d 142, 160 (3d Cir. 2004) ("In the context of Fed. R. Civ. P. 34(a), so long as the party has the legal right or ability to obtain the documents from another source upon demand, that party is deemed to have control."); Sixth Circuit - *In re Bankers Trust Co.*, 61 F.3d 465, 469 (6th Cir. 1995) ("[F]ederal courts have consistently held that documents are deemed to be within the "possession, custody or control" for purposes of Rule 34 if the party has actual possession, custody or control, or has the legal right to obtain the documents on demand."); Seventh Circuit - *Chaveriat v. Williams Pipe Line Co.*, 11 F. 3d 1420, 1427 (7th Cir. 1993) ("[T]he fact that a party could obtain a document if it tried hard enough and maybe if it didn't try hard at all does not mean that the document is in its possession, custody, or control; in fact it means the opposite."); Eighth Circuit - *Washam v. Evans*, 2011 U.S. Dist. LEXIS 70704, * 2 (E.D. Ark. 2011) ("A party may be ordered to produce a document in the possession of a non-party entity if that party has a legal right to obtain the document or has control over the entity who is in possession of the document."); Ninth Circuit *In re Citric Acid Litigation*, 191 F.3d 1090, 1107 (9th Cir. 1999) ("Control is defined as the legal right to obtain documents upon demand... Ordering a party to produce documents that it does not have the legal right to obtain will oftentimes be futile, precisely because the party has no certain way of getting those documents."); *See also* In re NCAA Student-Athlete Name & Likeness Litig., 2012 U.S. Dist Lexis 5087, at * 18 (N.D. Cal. Jan. 17, 2012) ("[t]his Court agrees with Magistrate Judge Paul S. Grewal [*Genentech, Inc. v. Trs. of the Univ. of Pa.*, 2011 U.S. Dist. 128526, *2 (N.D. Cal. 2011)], that the 'practical ability' test for 'control' [citation omitted] does not square with Ninth Circuit precedent"); *Super Film of Am., Inc. v. UCB Films, Inc.,* 219 F.R.D. 649, 651 (D. Kan. 2004)(""Control comprehends not only possession but also the right, authority, or ability to obtain the documents.' Therefore, Rule 34(a) enables a party seeking discovery to require production of documents beyond the actual possession of the opposing party if such party has retained 'any right or ability to influence the person in whose possession the documents lie.'").

b. Second Circuit - *Shcherbakovskiy v. Da Capo Al Fine, Ltd.*, 490 F.3d 130, 138 (2nd Cir. 2007) ("We also think it fairly obvious that a party also need not seek such documents from third parties if compulsory process against the third parties is available to the party seeking the documents. However, if a party has access and the practical ability to possess documents not available to the party seeking them, production may be required."); Fourth Circuit - *Morris v. Lowe's Home Ctrs*, 2012 U.S. Dist. LEXIS 44422, *20 (M.D.N.C. Mar. 29, 2012) ("A document is in a party's control when the party has 'the right, authority or practical ability to obtain the documents from a non-party to the action.'"); Fifth Circuit - *Wiwa v. Royal Dutch Petroleum Co.*, 392 F. 3d 812, 821 (5th Cir. 2004) ("The phrase 'to which he has access' is overbroad; it would require the retrieval of documents from Nigeria -- documents not under Oteri's custody, control, or possession, but to which he could conceivably have access by virtue of his prior position with Shell. We therefore limit the document request in the subpoena to documents within Oteri's custody, control, or possession."); *But see Exco Operating Co., LP v. Arnold*, 2011 U.S. Dist. LEXIS 138974 *20 (W.D. Louis. 2011) ("Rule 34's definition of 'possession, custody, or control,' includes more than actual possession or control of the materials; it also contemplates a party's 'legal right or practical ability to obtain the materials from a nonparty to the action.'");Eleventh Circuit - *Searock v. Stripling*, 736 F.2d 650, (11th Cir. 1984) ("Control is defined not only as possession, but as the legal right to obtain the documents requested upon demand....We do not, however, completely rest our holding on this factor of "control". We find instead that the primary dispositive issue is whether [the defendant] made a good faith effort to obtain the documents over which he may have indicated he had "control" in whatever sense, and whether after making such a good faith effort he was unable to obtain and thus produce them.").

c. First Circuit - *Velez v. Marriott PR Mgmt., Inc.,* 590 F. Supp. 2d 235, 258 (D.P.R. 2008) (the scope of the duty to preserve includes a duty to notify the opposing party of evidence in the hands of third parties); Second Circuit - *In re WRT* Energy *Secs. Litig.*, 246 F.R.D. 185, 195 (S.D.N.Y. 2007) ("If a party cannot fulfill [the] duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence"). *See also Cedar Petrochemicals, Inc. v. Dongbu Hannong Chem. Co.*, 769 F. Supp. 2d 269, 291 (S.D.N.Y. 2011) (the duty to preserve may be extinguished by provision to the opposing party of an "adequate and meaningful opportunity to inspect" the evidence); Sixth Circuit - *Jain v. Memphis Shelby County Airport Auth.*, 2010 U.S. Dist. LEXIS 16815 (W.D. Tenn. Feb. 25, 2010) (the scope of the duty to preserve includes a duty to notify the opposing party of evidence in the hands of third parties); Tenth Circuit - *Jordan F. Miller Corp. v. Mid-Continent Aircraft Serv.*, 139 F.3d 912 (10th Cir. 1998) (a party with possession of potentially relevant evidence has a duty to preserve it; even if the party relinquishes ownership or custody, it must contact the new custodian to preserve the evidence).

APPENDIX A: CHECKLISTS FOR DEVELOPING A BYOD PROGRAM

As discussed in the Report, a BYOD program may be the best way for a company to gain control of employees' use of personal devices and limit the risks. However, each employer must make its own decision based upon the sensitivity of the information its employees handle, whether the employer is in a highly regulated industry, the risk tolerance of the company, and its corporate culture. If a BYOD program is appropriate, then employers should consider the issues discussed in the Report. The checklist below contains a high-level summary of the recommendations set forth in the complete Report.

PLAN A BYOD PROGRAM

- Decide whether all employees should be permitted to participate in a BYOD program or whether certain groups should be excluded, such as senior executives, human resources staff, members of the legal department, sales staff, staff in research and development roles, contractors and contingent workers, and nonexempt staff, etc.
- If the company has unionized employees, determine whether the policy should extend to those employees, and if so, consult applicable collective bargaining agreements and labor counsel to develop a plan.
- If the company has employees outside the United States, plans should be made to address international issues such as privacy and data protection, reimbursement and tax obligations, and limits on working hours that may apply.

IDENTIFY TECHNICAL CONTROLS FOR DUAL-USE DEVICES

- Choose a Mobile Device Management (MDM) platform to manage employees' dual-use devices and identify the different types of mobile devices (and the specific versions of their operating systems) the MDM tool can support and manage.
- Limit the BYOD program to the specific devices and versions of operating systems the company can support with the MDM platform.
- Decide whether MDM software that creates a "sandbox" for company data is necessary to provide additional protections.
- Work with IT, Legal, HR, Security, and other relevant departments to configure the MDM tool to create appropriate security controls for dual-use devices, including, for example:
  - Encrypting all data stored on the device
  - Requiring strong passwords
  - Forcing the wipe of devices after 10 unsuccessful password attempts
  - Locking the device when idle
  - Prohibiting jailbroken devices
  - Prohibiting apps that contain malware
  - Locating the device if it is lost or stolen
  - Forcing the encryption of device backups

- Determine what data and services employees will be able to access with their dual-use devices. For example, will employees be limited to accessing work email, contacts, and calendars? Or will they also be able to establish a secure connection to the network to access additional applications or information? If broader access is desired, then evaluate whether virtualization technologies, like Citrix, will provide the desired functionality in a secure manner.

REVISE OR CREATE NEW POLICIES

Carefully review existing policies to identify changes that need to be made in light of the selected MDM software, access controls, device options, etc. At a minimum, companies should review the following policy areas.

Harassment, Discrimination, and Equal Employment Opportunities

- Clarify that company policies regarding harassment, discrimination, and retaliation apply to the use of dual-use devices and train all employees concerning proper and improper use.
- Train managers about how to respond to accommodation requests involving dual-use devices.

Workplace Safety

- Create an unequivocal policy statement that the company does not tolerate texting or talking on a hand-held device while operating a company vehicle or while operating a personal vehicle on company business.
- Educate employees about how to safely handle the need to text or talk while driving.

Recording Work Time

- Remind nonexempt staff to record all work time and revise policies if necessary to make this clear.
- Educate managers to be careful when sending e-mails and texts and making phone calls to nonexempt staff during off-hours.
- Evaluate options for employees to create unique ringtones or alerts to distinguish work and personal emails and calls to minimize the likelihood of claims for overtime or that employees were required to work off the clock.

Acceptable Use of Technology

- Clarify that company policies on acceptable use of technology apply to dual-use devices while on company time or on company premises.
- Educate employees about the care they should take to ensure that personal activities undertaken with dual-use devices must not intrude upon the workplace in a manner that violates other company policies, such as harassment, discrimination, etc.

Compliance and Ethics

- Clarify that company compliance and ethics obligations apply when using dual-use devices for work-related activities.

Privacy

- Clarify that employees using dual-use devices must provide access to their device upon demand for legitimate business purposes, such as an investigation or implementation of a litigation hold.

- Inform employees that the company may need to copy the entire device (including personal content) for litigation or investigations and then review and produce relevant materials to government agencies or third parties in litigation.
- Obtain employees' written consent to:
  - Review dual-use devices, including all data stored on and transmitted with them
  - Remotely wipe the device, including all work and personal information stored on the device
  - Install security software to manage the device and secure the data
  - Inspect the device and copy all data from the device (including personal data) to meet litigation hold and record retention obligations

Security

- Clarify that company security rules apply to dual-use devices and remind employees to follow good security practices when using their dual-use devices.
- Require employees to immediately report lost or stolen devices to ensure that "wipe" commands can be sent before devices lose battery power.
- Require employees to comply with configuration instructions and not to alter, bypass, or deactivate the operating system or other security features of the device without approval from senior management.
- Require employees to physically secure dual-use devices against theft, loss, or unauthorized use.
- Prohibit the use of dual-use devices by friends and family.
- Create policies to restrict employees from synchronizing or backing up the dual-use device in a way that would result in storing work-related data, such as with cloud-based services or applications that have not been approved for such use by the company's senior management.

Records Management and Litigation Holds

- Clarify that record retention, destruction, and litigation hold policies extend to work-related data stored on dual-use devices, as well as any third-party storage used by employees, such as cloud providers, online backup services, or home PCs that may have been used to synchronize or backup a dual-use device (in violation of any policy prohibiting such storage or synchronization of data).

Confidentiality and Trade Secret Protection

- Clarify that company policies regarding protection of trade secrets, private data, and confidential information apply to dual-use devices and educate employees about how to protect such information.

REQUIRE EMPLOYEE AGREEMENTS

- Create or modify existing employee agreements that employees must sign before being allowed to use a dual-use device to allow the company to assert control over its data after an employee has left the company.
- Consider whether claims relating to dual-use devices should be subject to an arbitration obligation.

DEVELOP NEW INTERNAL PROCESSES AND PROCEDURES

- Develop a group within the Information Technology Department with the skills and tools to effectively manage dual-use devices, including:
  - Tracking all dual-use devices used by employees
  - Secure configuration of dual-use devices
  - Use of the Mobile Device Management platform
  - Processes to remotely wipe data from dual-use devices
  - Tools and processes to forensically copy all data from the variety of dual-use devices used by employees
  - Monitoring and responding to new features and operating system updates for dual-use devices to maintain company controls
- Revise litigation hold policies and procedures to ensure dual-use devices are included within the scope of the company's litigation holds.
- Educate managers, IT staff, and legal counsel about the risks of accessing employee data stored in personal e-mail accounts and other online services and develop a policy for addressing such access.
- Develop new exit interview processes to ensure company data is preserved as necessary and then securely deleted from dual-use devices and any other storage areas used by employees, such as cloud-based storage services, home PCs that may have been used to synchronize or backup dual-use devices, etc.
- Review insurance coverages to determine whether existing insurance policies adequately address risks or whether additional coverages are available.
- Revise contingent worker contracts to address the use of dual-use devices.
- Evaluate employee reimbursement policies for the use of dual-use devices to address applicable laws.
- Develop a change management process to ensure company policies and procedures remain current and adequately mitigate the risks of dual-use devices as new applications and features are made available to employees.

EDUCATE EMPLOYEES

- Develop training and awareness programs for employees, managers, IT staff, and others to ensure they understand their role in appropriate use of dual-use devices and mitigation of the risks.

Littler Mendelson Offices

Albuquerque, NM
505.244.3115

Anchorage, AK
907.561.1214

Atlanta, GA
404.233.0330

Birmingham, AL
205.421.4700

Boston, MA
617.378.6000

Charlotte, NC
704.972.7000

Chicago, IL
312.372.5520

Cleveland, OH
216.696.7600

Columbia, SC
803.231.2500

Columbus, OH
614.463.4201

Dallas, TX
214.880.8100

Denver, CO
303.629.6200

Detroit, MI*
313.446.6400

Fresno, CA
559.244.7500

Gulf Coast
251.432.2477

Houston, TX
713.951.9400

Indianapolis, IN
317.287.3600

Kansas City, MO
816.448.3558

Las Vegas, NV
702.862.8800

Lexington, KY*
859.317.7970

Long Island, NY
631.293.4525

Los Angeles, CA
Downtown
213.443.4300

Los Angeles, CA
Century City
310.553.0308

Memphis, TN
901.795.6695

Miami, FL
305.400.7500

Milwaukee, WI
414.291.5536

Minneapolis, MN
612.630.1000

Morgantown, WV
304.291.3004

Nashville, TN
615.383.3033

New Haven, CT
203.974.8700

New York, NY
212.583.9600

Newark, NJ
973.848.4700

Northern Virginia
703.442.8425

Northwest Arkansas
479.582.6100

Orange County, CA
949.705.3000

Orlando, FL
407.393.2900

Overland Park, KS
913.814.3888

Philadelphia, PA
267.402.3000

Phoenix, AZ
602.474.3600

Pittsburgh, PA
412.201.7600

Portland, OR
503.221.0309

Providence, RI
401.824.2500

Reno, NV
775.348.4888

Rochester, NY
585.203.3400

Sacramento, CA
916.830.7200

San Diego, CA
619.232.0441

San Francisco, CA
415.433.1940

San Jose, CA
408.998.4150

Santa Maria, CA
805.934.5770

Seattle, WA
206.623.3300

St. Louis, MO
314.659.2000

Walnut Creek, CA
925.932.2468

Washington, D.C.
202.842.3400

INTERNATIONAL

Caracas, Venezuela
58.212.610.5450

Mexico City, Mexico
52.55.4738.4258

Monterrey, Mexico
52.81.8865.4340

*In Detroit, Littler Mendelson, PLC, in Lexington, Littler Mendelson, P.S.C., both are wholly-owned subsidiaries of Littler Mendelson, P.C.

Littler™

littler.com • Littler Mendelson, P.C.