A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.¹

Introduction

Lawyers and clients often communicate with each other via e-mail and sometimes communicate via other electronic means such as text messaging. The confidentiality of these communications may be jeopardized in certain circumstances. For example, when the client uses an employer’s computer, smartphone or other telecommunications device, or an employer’s e-mail account to send or receive e-mails with counsel, the employer may obtain access to the e-mails. Employers often have policies reserving a right of access to employees’ e-mail correspondence via the employer’s e-mail account, computers or other devices, such as smartphones and tablet devices, from which their employees correspond. Pursuant to internal policy, the employer may be able to obtain an employee’s communications from the employer’s e-mail server if the employee uses a business e-mail address, or from a workspace computer or other employer-owned telecommunications device on which the e-mail is stored even if the employee has used a separate, personal e-mail account. Employers may take advantage of that opportunity in various contexts, such as when the client is engaged in an employment dispute or when the employer is monitoring employee e-mails as part of its compliance responsibilities or conducting an internal investigation relating to the client’s work.² Moreover, other third parties may be able to obtain access to an employee’s electronic communications by issuing a subpoena to the employer. Unlike conversations and written communications, e-mail communications may be permanently available once they are created.

The confidentiality of electronic communications between a lawyer and client may be jeopardized in other settings as well. Third parties may have access to attorney-client e-mails when the client receives or sends e-mails via a public computer, such as a library or hotel computer, or via a borrowed computer. Third parties also may be able to access confidential communications when the client uses a computer or other device available to others, such as when a client in a matrimonial dispute uses a home computer to which other family members have access.

In contexts such as these, clients may be unaware of the possibility that a third party may gain access to their personal correspondence and may fail to take necessary precautions. Therefore, the risk that third parties may obtain access to a lawyer’s e-mail communications with a client raises the question of what, if any, steps a lawyer must take to prevent such access by third parties from occurring. This opinion addresses this question in the following hypothetical situation.

An employee has a computer assigned for her exclusive use in the course of her employment. The company’s written internal policy provides that the company has a right of access to all employees’ computers and e-mail files, including those relating to employees’ personal matters. Notwithstanding this

¹ This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2011. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.
² Companies conducting internal investigations often secure and examine the e-mail communications and computer files of employees who are thought to have relevant information.
policy, employees sometimes make personal use of their computers, including for the purpose of sending personal e-mail messages from their personal or office e-mail accounts. Recently, the employee retained a lawyer to give advice about a potential claim against her employer. When the lawyer knows or reasonably should know that the employee may use a workplace device or system to communicate with the lawyer, does the lawyer have an ethical duty to warn the employee about the risks this practice entails?

**Discussion**

Absent an applicable exception, Rule 1.6(a) requires a lawyer to refrain from revealing “information relating to the representation of a client unless the client gives informed consent.” Further, a lawyer must act competently to protect the confidentiality of clients’ information. This duty, which is implicit in the obligation of Rule 1.1 to “provide competent representation to a client,” is recognized in two Comments to Rule 1.6. Comment [16] observes that a lawyer must “act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.” Comment [17] states in part: “When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.... Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.”

This Committee has recognized that these provisions of the Model Rules require lawyers to take reasonable care to protect the confidentiality of client information, including information contained in e-mail communications made in the course of a representation. In ABA Op. 99-413 (1999) (“Protecting the Confidentiality of Unencrypted E-Mail”), the Committee concluded that, in general, a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating Model Rule 1.6(a) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The opinion, nevertheless, cautioned lawyers to consult with their clients and follow their clients’ instructions as to the mode of transmitting highly sensitive information relating to the clients’ representation. It found that particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.

Clients may not be afforded a “reasonable expectation of privacy” when they use an employer’s computer to send e-mails to their lawyers or receive e-mails from their lawyers. Judicial decisions illustrate the risk that the employer will read these e-mail communications and seek to use them to the employee’s disadvantage. Under varying facts, courts have reached different conclusions about whether an employee’s client-lawyer communications located on a workplace computer or system are privileged, and the law appears to be evolving. This Committee’s mission does not extend to interpreting the substantive law, and

---

3 See, e.g., ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 08-451 (2008) (Lawyer’s Obligations When Outsourcing Legal and Nonlegal Support Services) (“the obligation to ‘act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision’” requires a lawyer outsourcing legal work “to recognize and minimize the risk that any outside service provider may inadvertently -- or perhaps even inadvertently -- reveal client confidential information to adverse parties or to others who are not entitled to access ... [and to] verify that the outside service provider does not also do work for adversaries of their clients on the same or substantially related matters.”).

therefore we express no view on whether, and in what circumstances, an employee’s communications with counsel from the employee’s workplace device or system are protected by the attorney-client privilege. Nevertheless, we consider the ethical implications posed by the risks that these communications will be reviewed by others and held admissible in legal proceedings. Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of e-mail communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others. In particular, as soon as practical after a client-lawyer relationship is established, a lawyer typically should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.

The time at which a lawyer has an ethical obligation under Rules 1.1 and 1.6 to provide advice of this nature will depend on the circumstances. At the very least, in the context of representing an employee, this ethical obligation arises when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party. Considerations tending to establish an ethical duty to protect client-lawyer confidentiality by warning the client against using a business device or system for substantive e-mail communications with counsel include, but are not limited to, the following: (1) that the client has engaged in, or has indicated an intent to engage in, e-mail communications with counsel; (2) that the client is employed in a position that would provide access to a workplace device or system; (3) that, given the circumstances, the employer or a third party has the ability to access the e-mail communications; and (4) that, as far as the lawyer knows, the employer’s internal policy and the jurisdiction’s laws do not clearly protect the privacy of the employee’s personal e-mail communications via a business device or system. Unless a lawyer has reason to believe otherwise, a lawyer ordinarily should assume that an employer’s internal policy allows for access to the employee’s e-mails sent to or from a workplace device or system.

The situation in the above hypothetical is a clear example of where failing to warn the client about the risks of e-mailing communications on the employer’s device can harm the client, because the employment dispute would give the employer a significant incentive to access the employee’s workplace e-mail and the employer’s internal policy would provide a justification for doing so. The obligation arises once the lawyer has reason to believe that there is a significant risk that the client will conduct e-mail communications with the lawyer using a workplace computer or other business device or via the employer’s e-mail account. This possibility ordinarily would be known, or reasonably should be known, at the outset of the representation. Given the nature of the representation—an employment dispute—the lawyer is on notice that the employer may search the client’s electronic correspondence. Therefore, the lawyer must ascertain, unless the answer is already obvious, whether there is a significant risk that the client will use a business e-mail address for personal communications or whether the employee’s position entails using an employer’s device. Protective measures would include the lawyer refraining from sending e-mails

See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-460 (2011) (Duty When Lawyer Receives Copies of a Third Party’s E-mail Communications with Counsel).
to the client’s workplace, as distinct from personal, e-mail address,7 and cautioning the client against using a business e-mail account or using a personal e-mail account on a workplace computer or device at least for substantive e-mails with counsel.

As noted at the outset, the employment scenario is not the only one in which attorney-client electronic communications may be accessed by third parties. A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client’s situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.

7 Of course, if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer or other device owned or controlled by the employer, then a duty arises to caution the client not to do so, and if that caution is not heeded, to cease sending messages even to personal e-mail addresses.
A California Court of Appeal recently issued a short decision in Cochran v. Schwan's Home Services, Inc., B247160 (Aug. 12, 2014) that took an expansive view of an employer’s obligation to reimburse employees for business expenses. In light of this decision, employers should conduct a careful and wide-ranging review of their reimbursement policies and take a hard look at what actually happens “in the field.”

The plaintiff, who worked as a customer service manager, sued his employer to recover expenses for the work-related use of his personal cell phone. The plaintiff asked the court to certify his case as a class action. The trial judge denied class certification on the ground that individualized inquiries about the class members’ cell phone plans would overwhelm common issues. In effect, the trial court determined that no “expense” was incurred, and no reimbursement owed, unless the employee had to pay something out of pocket, above and beyond the expense to maintain the cell phone for personal use. The appellate court disagreed, finding that an employer is obligated to reimburse an “expense,” even if the employee has incurred no additional cost associated with the business use of the phone. Because this error was the basis for the trial court’s decision to deny certification, the court reversed that decision and sent the case back to the trial court.

The Obligation to Reimburse Business Expenses

California Labor Code section 2802 obligates employers to reimburse employees for “all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties, …” The Cochran decision posed, and answered, the “threshold question” presented on appeal as follows:

Does an employer always have to reimburse an employee for the reasonable expense of the mandatory use of a personal cell phone, or is the reimbursement obligation limited to the situation in which the employee incurred an extra expense that he or she would not have otherwise incurred absent the job? The answer is that reimbursement is always required. Otherwise the employer would receive a windfall because it would be passing its operating expenses onto the employee.
Based on this interpretation of section 2802, the Cochran court found the trial court erred when it determined that the obligation to reimburse would depend on (1) whether the employee had a plan allowing unlimited use; and (2) whether the employee or a family member paid the bill. Instead, it held that when an employee “must” use his personal cell phone for work-related calls, the employer must reimburse him and that the “reimbursement owed is a reasonable percentage of the cell phone bills.”

The court’s language strongly suggests that an employer must reimburse an employee any time the employee is required to provide a benefit to the employer that could fall into the category of “operating expenses.” This is true whether the benefit is provided directly by the employee (his own cell phone which he pays for himself) or by a third party (a family member who pays the bill).

Indeed, the court pointed out that its broad interpretation of section 2802 not only prevents employers from passing on operating expenses, but also “prevents them from digging into the private lives of their employees to unearth how they handle their finances vis-à-vis family, friends and creditors,” making clear its dismissal of the theory that “who paid the bills” is of any consequence.

The case most heavily relied upon by the Cochran court was its own prior decision in a case involving reimbursement for business use of an employee’s car. In calculating the appropriate amount of reimbursement in that case, the court recognized that the employee was not just buying gas for the car, but the car itself, which had to be insured, and was subject to wear and tear, resulting in diminished value.

Arguably, the principles derived from prior cases may not work well when applied to reimbursement for the use of other kinds of employee property. A cell phone is not analogous to a car. The employee’s car is, in a real sense, a consumable asset; his cell phone much less so. The “asset” of home access to the Internet, to support use of a tablet or computer, is not in the least diminished by its use, although data usage caps may apply. The different quality of the various personal assets that may be used for a business purpose may call for a more nuanced approach to sensibly fulfill the purpose of section 2802: to forbid employers the “windfall” of passing on their operating costs to their employees. It seems certain that Cochran will generate its share of litigation.

The Class Action Ruling

Notably, the Cochran appellate court did not order the trial court to certify the class. Rather, it ordered the trial court to reconsider the motion, to apply the rulings on the proper interpretation of section 2802, and apply the principles recently announced by the California Supreme Court in Duran regarding statistical sampling. It specifically provided that the plaintiff could revise his motion and the defendant could respond. Perhaps the parties and the trial court will take the opportunity to examine whether common questions are outweighed by individual issues needed to prove whether use of personal cell phones for work calls was a “must” (i.e., required by the employer), or just the employee’s choice.

The decision suggests that the court may have recognized the need to develop the factual record and/or the trial court’s analysis of the very open question of when an employee’s use of a personal cell phone becomes a “must.” While the court announced sweeping principles that come into play when an employee “must” use a personal cell phone (or other items) for the employer’s benefit, it offered neither information nor analysis about what evidence will be enough to prove that the use of a personal asset for business purposes is a “must.”

Moreover, the court noted that, in making decisions about reimbursement of expenses, employers 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.” (Emphasis added.)

In the absence of a direct employer mandate to use personal cell phones or furnish other items for the employer’s benefit, this standard may well require examination of a wide range of individualized factors in order to determine whether the employer is obligated to reimburse a particular employee for any particular business expense. That could be an alternate reason, not cited by the trial court, for a determination that class certification of the plaintiff’s claims was not appropriate.

2  See Kevin Lilly, California Supreme Court Stabilizes the Law in California Misclassification Class Action Cases, Littler ASAP (Jun. 2 2014).
The Take-away

The principles announced in Cochran are not limited to personal cell phones. They may apply, with equal force, to many other “personal” items that stock most modern households. Personal laptops, “tablets,” the Internet connections to use them, and even the humble dinosaur of a home land-line phone, could all, at least theoretically, be the subject of claims for reimbursement under these principles.

Employers should very carefully review their policies and practices regarding reimbursement of business expenses. They should determine how their managers and supervisors communicate with employees and what “expectations” are set, not just by written policies, but in practice. Employers should consider making those expectations concrete by putting them in writing. They should make sure their managers, supervisors, and employees all understand the reasons for the policies and the consequences of not following them.

If cell phone communications are required, employers should consider supplying company-owned phones. Doing so will make it clear that use of personal phones is not mandatory. It will also minimize the court’s concerns about intrusion into employee privacy. If the employer owns the phone and maintains appropriate policies on the use of electronic media, it will also maximize its rights to monitor cell phone usage.

Of course, the same principle applies if an employer requires its employees to have access to a computer or tablet device away from its premises. It is well-established that, subject to proper policies, an employee does not have a reasonable expectation that what he or she creates, stores, receives, or sends from a company-owned computer is private and can be kept from the gaze of the company.

If access to a computer at the employee’s home is required on a frequent basis, employers may wish to consider providing an employer-owned mobile “hot spot” available to its employees to avoid a claim that the employer must pay for some ill-defined percentage of the cost of the employee’s choice in home Internet access.

Employers should also think about their workplace practices to identify any sort of personal assets that employees may use for their jobs in order to make reasoned decisions about how to manage the issues raised by Cochran.

Diane Kimberlin is a Shareholder in Littler’s Los Angeles (Century City) office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, or Ms. Kimberlin at dkimberlin@littler.com.
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
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.

Copyright ©2012 Littler Mendelson, P.C.
All material contained within this publication is protected by copyright law and may not be reproduced without the express written consent of Littler Mendelson.
# Table of Contents

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

---


• **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.

### 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. 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. 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

---


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.


\(^8\) Id.

\(^9\) Id.

\(^10\) Id.


\(^12\) JP Finnell, Transient Apps: The Consumer Influence on Enterprise Mobility, Part 2, GigaOm, Aug. 2010.


\(^14\) 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.  

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 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.

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?”

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. 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.

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.” 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.
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.\textsuperscript{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.

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

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

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

---


29 See 45 C.F.R. pts. 160, 162 and 164.
obtained seven-figure settlements in two different matters arising from security breaches.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{33}

Other states, such as California and Texas, impose a general statutory duty on businesses to safeguard personal information.\textsuperscript{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.\textsuperscript{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—such as, 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

\textsuperscript{34} See CAL. CIV. CODE §§ 1798.80 et seq.
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

---

38 See 45 C.F.R. pt. 164.312(a)(2), (e)(2).
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. 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. 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. 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., 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. Similarly, and as one example, if an employer uses the employee’s dual-use device to access

---

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.
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 “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., 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.” Notably, to date, Stengart has not yet been followed
in any other jurisdiction.

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
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. 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). 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 is not surprising given that reported e-Discovery sanctions cases continue to dominate legal headlines, 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).

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.

Moreover, despite the fact that certain, baseline e-Discovery standards and litigation support technologies are—seven years after Zubulake—well established, 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. In today's digital world, this requires having a thorough understanding of an employer's data infrastructure, 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, 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 proportional, this year it is computer-assisted coding, often generally 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.”)


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. 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.

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.” 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.

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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Rule 34 Definition of “Control”</th>
<th>Circuit Courts that follow this test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 1</td>
<td>A party must produce information that it has the legal right to obtain on demand.</td>
<td>District of Columbia, 1st, 3rd, 6th, 7th, 8th, 9th, and 10th Circuits.</td>
</tr>
<tr>
<td>Category 2</td>
<td>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.</td>
<td>2nd, 4th, 5th, and 11th Circuits.</td>
</tr>
<tr>
<td>Category 3</td>
<td>In addition to the above, these Circuits require a party to notify its adversary about evidence in the hands of third parties.</td>
<td>1st, 2nd, 6th, and 10th Circuits.</td>
</tr>
</tbody>
</table>

[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).
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. 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. Accordingly, the employee has no right to use the information for his personal purposes, absent the employer's consent and must surrender the information upon demand absent a transfer of ownership or possession.

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. 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. 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.

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. 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. 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 employee's 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).
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. Accordingly, the newspaper did not have the legal right to obtain the flash drive over the reporter’s objection.

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. 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. 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.

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?

Moreover, as discussed above, employers may face civil and criminal 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. 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.

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. Thus, if an adversary demands such information in discovery, an employer can and should object, 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

See e.g., When Custodians Could be Culprits, N.Y.L.J., Adam Cohen and Maureen O’Neil, Oct. 27, 2008.
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).
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.).
See In re Grand Jury Subpoenas, 722 F.2d at 986 (2d Cir. 1983).
It is fair game to demand the preservation and production of data from plaintiffs’ personal computers, e-mail accounts, PDAs 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/PublicArticleTN.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 employee’s 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.

---

89 Id.
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 when it is reasonably necessary to accomplish the purpose of his employment and in furtherance of the master’s business.”).
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.” 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). 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. 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.


95 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."  

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. While having a policy or non-contractual document regarding confidentiality is helpful, the more recognized practice is to enter into confidentiality agreements with employees. 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 of counsel.

---

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.").
of counsel. 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. 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. Samso, 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 was not subject to 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).

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. 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.”

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. 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.


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

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. 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,
sex, and religion;\textsuperscript{107} veteran status;\textsuperscript{108} genetic information;\textsuperscript{109} pregnancy;\textsuperscript{110} age;\textsuperscript{111} physical or mental disability;\textsuperscript{112} and require reasonable accommodation of qualified people with disabilities.\textsuperscript{113} Some states and local governments are even more expansive, e.g., prohibiting discrimination based on sexual orientation,\textsuperscript{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.\textsuperscript{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.\textsuperscript{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 \textit{Blakey v. Continental Airlines, Inc.},\textsuperscript{117} a female pilot complained of a sexually hostile work environment based upon the content

\textsuperscript{107} Title VII of the Civil Rights Act of 1964 (Title VII), 42 U.S.C. §§ 2000e et seq.
\textsuperscript{108} Uniformed Services Employment and Reemployment Rights Act, 38 U.S.C. §§ 4301 et seq.
\textsuperscript{109} Genetic Nondiscrimination Act, 42 U.S.C. §§ 2000ff et seq.
\textsuperscript{111} Age Discrimination in Employment Act of 1967, 29 U.S.C. §§ 621 et seq.
\textsuperscript{113} ADA, 42 U.S.C. §§ 12101 et seq.
\textsuperscript{114} See, e.g., 42 U.S.C. § 2000e-3(a) (Title VII).
\textsuperscript{116} See, e.g., 42 U.S.C. § 2000e-3(a) (Title VII).
\textsuperscript{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, 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.” 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.” 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....” 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. 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.

119 Id. at 5.
120 Id. at 12 (quoting Blakey, 751 A.2d at 543).
121 Id. (quoting Blakey, 751 A.2d at 552).
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 devices125.

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

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.
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 hardship134 defense to the general obligation to
accommodate a qualified person with a disability. But generalized conclusions about undue hardship are insufficient.

---

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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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

\textsuperscript{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).

\textsuperscript{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”).

\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{144}

\textsuperscript{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.

\textsuperscript{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.

\textsuperscript{143} 29 C.F.R. §§ 531.35; 531.36; 531.37.

\textsuperscript{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.

---

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. 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.

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.

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. 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 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 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.”

The traveler’s consent is not required for the search. Further, asserting that the information is protected against disclosure under the attorney-client privilege will not necessarily exempt the data from the search. The Directives guide the officers to consult with the agency’s legal counsel or the local attorney’s office before proceeding with the search. 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. Finally, the agent may detain the device for days to complete a “thorough border search,” which could cause major inconvenience.

---

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, 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.

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.

---

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 not165) 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,
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. 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.

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
- 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 For example, an Apple publication entitled Deploying iPhone and iPad Mobile Device Management describes the many options available for configuring Apple’s iOS devices, including iPhones and iPads is available at http://images.apple.com/iphone/business/docs/iOS_MDM.pdf.
168 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 synchronization 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 “LITTLE” 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, 360 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.3d 650, 652 (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 Hanhong 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  
213.443.4300

Los Angeles, CA  
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  
479.582.6000

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  
415.432.1940

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.
When “secure enough” isn’t enough:
A Law Firm Guide to Protecting the Confidentiality of Shared Client Files

Christopher T. Anderson, JD
Product Manager, LexisNexis

Dan Barahona, SVP
Strategy & Business Development,
WatchDox
In 2012, 90% of IT respondents said their organization had experienced a breach of document security.1
When “secure enough” isn’t enough

When it comes to sharing confidential documents with clients or authorized third parties, law firms have traditionally faced a choice between two competing interests: usability or security, seldom both.

Easy choice. Ask for a show of hands among attorneys and security will win out every time. After all, maintaining client confidentiality is a cornerstone of ABA rules governing attorney behavior:

**Model Rules of Professional Conduct 1.6:**
Confidentiality of Information
(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

So why is it that so many attorneys today still use traditional file-sharing methods such as email or even fax, along with USB thumb drives or consumer online file-sharing sites? At its most basic, there may be a divide between what firms think is secure, and what actually is secure.

This paper offers up some of the best alternatives today and hopefully provides insights to help you clear up any confusion.

Now that enterprise file-sharing solutions featuring simple drag-and-drop interfaces are on the market, it may no longer be necessary to make a choice between usability and security, though with that term “enterprise” may come a third concern: affordability.

Before we get ahead of ourselves, though, it’s worth taking a hard look at why security is taking center stage in the debate about file-sharing methods, not just in the legal market, but for every type of organization.

---

1 Source: Ponemon Institute study: “2012 Confidential Documents at Risk Study”
Comparatively speaking, law firms – especially small to midsize ones – are soft targets for data thieves. They can be easy to break into – physically and electronically – and they have very valuable information such as social security numbers to go along with names and addresses.

That’s not even to mention all the other confidential information – medical documents, tax and financial records, intellectual property, data about potential mergers and acquisitions... all types of information that can be used against your clients in any number of ways, none of them good.

Any attorney that plays a part in allowing confidentiality to be compromised, however unintentional it may be, is at risk of being held responsible. And the risk is only getting worse. Between 2008 and 2011, malpractice claims rose 30% over the previous four-year period.²

Considering that the category “Preparation, Transmittal or Filing of Documents” is historically the number one legal category cited in malpractice claims³, you owe it to everyone concerned to thoroughly investigate just how secure different document sharing options really are.

Let’s start with some of the more basic, old-fashioned tools in use today for sending documents to legal clients and authorized third parties.
Email, thumb drives, consumer file-sharing sites...
Why good enough may not be good enough anymore.

Life is a lot easier when we stick with what we know. Unfortunately, what many attorneys don’t know about the security of different document transmission methods is getting in the way of properly protecting their clients’ needs for confidentiality.

The ABA has taken a stand about your responsibility as an attorney to stay updated about the strengths and weaknesses of different technology options:

---

**Model Rules of Professional Conduct 1.1: Competence**

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.

---

Following are some of the more common file-sharing solutions in use today and why they might not be as secure as you’ve allowed yourself to think.

**Email**

Other than the telephone, there may be no other way of remotely connecting with others that has had such a positive impact on our lives as email.

Unfortunately, that positive impact can quickly turn into a head-on collision when client confidentiality is at stake.

In a 2012 survey of IT professionals from all types of organizations, the Ponemon Institute found that [71% of respondents said that their organization likely or very likely had experienced a theft or loss of email attachments.](#)

---

1 Source: Ponemon Institute study: “2012 Confidential Documents at Risk Study”

2 Source: “ABA Profile of Legal Malpractice Claims” (2011 Study)
Because of email’s security vulnerabilities, the ABA Standing Committee on Ethics and Professional Responsibility has issued a formal opinion specifically addressing it and other electronic document transmission methods:

Formal Opinion 11-459: “Duty to Protect the Confidentiality of E-Mail Communications with One’s Client”
A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access...

What are some of the email security issues attorneys should be aware of? Email can:

1. Be read and intercepted at:
   a. Router points
   b. Internet service provider (ISP)
   c. Internal IT departments
2. Be inadvertently sent to the wrong recipient
3. Be forwarded to unauthorized recipients
4. Be printed, then read by unauthorized recipients
5. Be accidentally caught up in litigation holds
6. Get lost in spam filters
Of course, there are ways to make email transmissions more secure, and we don’t mean the disclaimer language most businesses add at the end of their emails.

One way to protect email contents is with encryption, which can definitely be worth your while to investigate if you’re adamant about sticking with email for sending confidential documents. You still need to be aware, though, that encryption doesn’t protect against copying, forwarding and downloading once the message has been decrypted. It also requires recipients to go through the decryption process to read your message, so not every client will have the sophistication necessary to decode encrypted email.

**USB thumb/flash drives**

Many attorneys use thumb drives both as a way to share documents, and to take work home or transfer files when they’re traveling. They’re small. They’re convenient. And according to the application the file is created on, they can be read by almost anyone.

On the downside: They’re small, making them easy to lose, steal or forget. They’re convenient, so their use has become commonplace. And, of course, they can be read by almost anyone, including thieves and others who may inadvertently find them.

In fact, that same Ponemon Institute survey cited previously found that USB drives were just behind email in their lack of security:

68% of IT respondents reported that they likely or very likely had experienced a theft or loss of data stored on a USB drive.¹

¹ Source: Ponemon Institute study: “2012 Confidential Documents at Risk Study”
Consumer file-sharing options

Consumer online file-sharing options have reinvented the way many of us think about sending files and collaborating with others. Ease of use has made such services wildly popular among the general public for sharing everything from pictures of new babies and puppies to the latest discovery about outer branches of the family tree.

There is a dark side to this wonderful capability, though: Consumer file-sharing services were never created with the intention of protecting the kind of confidential information lawyers pass on to their clients and opposing counsel. The security protections were never put in place to safeguard business-critical files, much less meet the confidentiality requirements of law firms.

Part of the problem is how easy it is to share not just a file or two, but thousands of files in a matter of seconds. There have been horror stories of attorneys attempting to share specific folders with opposing counsel, only to later realize that they made every folder on their computers accessible as well.

Because they’re so easy to use and seemingly harmless, many users are simply unaware of the threat to security consumer file-sharing solutions can create.

3 Source: “Catching Up to the Cloud: Steady migration into cloud-based file-sharing, email, and productivity services”, a Spiceworks Market Insights Report, June, 2013

4 Source: “Security Considerations for Online File-sharing” (Terri McClure, Senior Analyst and Kristine Kao, Associate Analyst) Enterprise Strategy Group
In a June, 2013 report, a Spiceworks Market Insights survey of over 500 IT professionals from small and midsize organizations found that half said their employees were already using cloud-based file-sharing services on their own.3 In a March, 2013 white paper, Enterprise Security Group said that:

70% of IT managers surveyed “know or believe that users have business data in their own personal file-sharing accounts.”4

From a practice perspective, it’s entirely possible for your firm to lose access to your own data if an employee leaves without first notifying you where files are stored.

From an IT perspective, the problem has gotten so bad that some firms are now prohibiting the use of consumer file-sharing sites.

Whatever your firm is considering, it’s essential to study your options – along with the Terms & Conditions and Privacy Policy of each – to know exactly what you’re getting. If you have colleagues using free file-sharing accounts, you need to be aware that the providers of those accounts may assert ownership rights over client or firm files.
Public computers

Every attorney knows better than to think a public computer is secure in any way. But not all clients will be aware of the dangers, so make sure that they’re also informed of the risks. No public computer, whether it’s at a library, business center, hotel, airport, etc. offers adequate protections against privacy or security breakdowns.

Make sure, too, that your clients understand the limitations of privacy on their employers’ computers. Especially in a consultation or case involving an employer dispute, it’s important to remind clients that many companies have policies giving employees no reasonable expectation of privacy for anything found on their company computers.

Fax

While advances in technology have given us much better and more secure ways to share important information, you may still have clients who insist on sending documents to your office by fax. While you should warn them about the inherent lack of security, you should also take precautions such as putting the machine in direct proximity to a scanner and shredder. That way, you’ll be able to scan documents into your practice management software on the spot, then safely dispose of the originals.
Laptops/desktops/portable/back-up drives

Almost all of us use laptops and desktops on a regular basis, but we’re not necessarily as careful as we need to be about protecting confidential data on them.

Make sure that all firm computers and portable back-up/hard drives are protected with passwords that include upper and lower case letters, numbers and symbols. Having a strong password is a good first step, but by no means is it the final word on your responsibilities.

Full-disk encryption is an easy way to protect confidential data. According to a late 2012 article in GPSolo, encryption can be “so effective that law enforcement and federal agencies are complaining that they are unable to retrieve encrypted data in criminal investigations.”5

Keep in mind, too, that even disabled and discarded computers or photocopiers can put your firm at risk of exposing confidential client data. Before you dispose of electronic devices, even hopelessly outdated or out-of-service devices, make sure the storage media are destroyed.

Mobile/bring your own devices (BYOD)

For years, law firms and other security-conscious organizations have had legitimate concerns about the confidentiality of data stored on their own smartphones and tablets; even more so over the use of their employees’ own devices.

Mobile devices are of particular concern because they’re exactly that: mobile. They’re easy to lose track of, easy to steal, and even people trying to be helpful may stumble on confidential data if it’s stored on the device.

While it’s essential to protect electronic devices with strong passwords and learn how to wipe a lost smartphone or tablet, you’re even safer if confidential data isn’t stored on the device.

Which brings us to... The Cloud.

5 Source: GPSolo, November/December 2012, “Encryption Made Simple for Lawyers” by David G. Ries and John W. Simek
Not all clouds are created equally.

In travelling around the country speaking to lawyers about document security, we almost invariably come across attorneys who are adamant about refusing to use cloud services, assuming they’re the opposite of secure, sometimes with very good reason.

After all, the consumer file-sharing solutions we talked about earlier built their business models on moving documents from one user to another by way of the cloud, and we’ve already discussed the risks they pose to law firms.

Fortunately, all is not lost. Depending on which version of the cloud you’re using, there are more secure online file-sharing (OFS) options out there.
What about “Enterprise” versions of consumer file-sharing solutions?

We’ve made our point about the dangers of using consumer online file-sharing options for protecting confidential client documents or information.

Any firms still willing to put their trust in such solutions are putting their confidentiality obligations at risk, along with the trust of their clients. If a security breakdown is egregious enough, there may even be grounds for a malpractice suit or ABA sanctions.

Today, though, many of those same consumer OFS companies are offering what they refer to as “Business” or “Enterprise” file-sharing versions of their consumer solutions. Some, in fact, have invested heavily in beefing up security for enterprise OFS solutions with high-grade options such as encrypting data on transfer with 256-bit SSL and at rest with 256-bit AES.

For security-conscious law firms, that’s a welcome addition for safeguarding client confidentiality. Enterprise or business versions are not free like their consumer cousins, but with several options available, it may be worth shopping around to compare security, storage limits and prices before making a final decision.

As long as you’re being thorough, though, it’s worth looking further in your search for the most secure file-sharing options.
If security is your number one priority, consider a solution built with security as its priority.

In addition to investigating consumer solutions with “bolt-on” security added to create so-called enterprise versions, you should also look into services that offer the same drag-and-drop ease of use, but that were created from the ground up with security as the first priority.

That’s not to say it’s impossible to make consumer file-sharing options safe for enterprise use; it’s just that bolt-on security will almost always be just that, an add-on usually created in response to known security breaches.

If maintaining confidentiality is top-of-mind, it only makes sense to investigate file-sharing solutions that started with security in mind.

Certain solutions such as WatchDox®, for instance, take an entirely different approach to protecting confidential files, embedding security into the documents themselves. Even documents downloaded to a device that is later lost or stolen will be unreadable to anyone except authorized users.
By applying controls at the file level, such solutions allow users to protect document security through the entire lifecycle of the file, so they can:

- Define who is allowed to access a document
- Control how a file is viewed and duplicated, including the ability to allow or block printing, editing, copying and forwarding
- Set expiration dates, or revoke permission to view a document at will
- Create an audit trail of where documents were viewed, on which devices and at what times

It’s not hard to see how a document-centric security solution could be a great tool for helping uphold ABA confidentiality requirements.

Estate attorneys could send clients drafts of their wills without concern that another family member might come across it accidentally, or even dig through family computers searching for such documents. Corporate firms could protect their clients from having confidential documents copied or forwarded by well-meaning (or not) insiders. And any type of lawyer could go back to downloading protected documents onto thumb drives, smartphones or tablets without concern.

From a security standpoint, that’s a game-changer. In fact, Gartner and Forrester analysts agree that WatchDox is the most secure enterprise file-sharing solution in the marketplace. But because it was originally created for the Fortune 100, attorneys haven’t had the kind of access to WatchDox as they have to consumer file-sharing sites.

All that changed in the fall of 2013 when LexisNexis® created a strategic partnership with WatchDox to provide enterprise-secure file-sharing at no extra cost with the latest versions of Time Matters® and LexisNexis Firm Manager® practice management programs.
If in doubt, take a test drive

It’s simply not reasonable, or even possible, to search and investigate all the OFS options out there. In fact, you could probably spend months searching and studying solutions and still not reach the end of the list.

All is not lost, though. If you’re having a difficult time narrowing your choices, choose a couple of options and compare them against each other. All the OFS solutions we found give you the option to try or demo them free for a limited time, including the document security powered by WatchDox, along with the Time Matters and LexisNexis Firm Manager practice management programs that include it.

If your firm specializes in a specific type of law, you’ll also want to check for applicable certifications. For instance, if you do a lot of medical work, make sure any solutions you consider have achieved HIPAA and HITECH certifications. In the same way, if your firm works with financial or securities organizations, you should seek out OFS solutions with GLBA certification.

Your firm will have the security of knowing that your file-sharing solution has met the strict standards of the agency that oversees such programs, and potential clients will have the assurance that your firm takes the security of their confidential information seriously.

Such certifications may also help answer any security questions that may arise during the resolution of a matter.
Christopher T. Anderson, JD

Prior to his present position as Product Manager for LexisNexis Firm Manager®, Christopher Anderson built a distinguished legal career during which he developed the expertise he now uses in his job at LexisNexis®, and in frequent seminars on this and other topics related to helping attorneys build better practices through technology.

Anderson’s legal background includes stints as:

• Managing Partner for an eight-attorney full-service law firm in Georgia, at which he specialized in family law and business litigation
• Assistant District Attorney in New York City, and in Athens, Georgia
• Associate General Counsel and Director of Client Services for RealLegal (Law.com)

Christopher graduated from Cornell University and earned his Juris Doctorate from the University of Georgia School of Law in 1994. He is admitted to practice in the federal and state courts of New York and Georgia.

Dan Barahona

Dan Barahona leads business development for WatchDox® and is responsible for the company’s strategic partnerships and driving new market opportunities. Before joining WatchDox, Dan was Vice President of Business Development at ArcSight™, where he led the company’s technology alliances and partner ecosystem, as well as their integration into HP after its acquisition. Prior to ArcSight, Dan was one of the first 10 employees at Sensage® and drove the company’s transformation into the information security space. As the Vice President of Business Development, Dan led strategic alliances at Sensage, completing OEM relationships with HP and Cerner, and partnerships with EMC, McAfee and SAP.

Dan holds a B.S. degree in Engineering from the Rensselaer Polytechnic Institute in Troy, New York, a Master of Engineering degree from Cornell University, and an MBA from the University of Michigan.
LexisNexis® Law Firm Practice Management Products

Time Matters® software is an award-winning practice management program that maintains and connects all of your client, case and document data in one instantly searchable database. The latest version includes WatchDox® technology, which gives small and midsize law firms enterprise-secure online file-sharing at no extra charge with their annual maintenance plan subscriptions.

LexisNexis Firm Manager® web-based software is an easy, secure, online practice management program made for solo attorneys and small law firms that enables you to be the lawyer you dreamed of being. The LexisNexis Firm Manager program includes WatchDox® technology for enterprise-secure, drag-and-drop easy document sharing.

PCLaw® software is an all-in-one matter and financial management program for small to midsize law firms. PCLaw 13 dashboards give you a lawyer’s-eye view of what’s most important to your practice, your clients and your business, so you can get on top of your entire day over your first cup of coffee.

Juris® software is a legal-specific billing, accounting and financial management program that not only helps firms take control of their everyday billing and accounting needs; it can actually help increase profitability by giving practice owners and partners the in-depth insights they need to measure and improve firm operations.

www.lexisnexis.com/lawpractice
I. INTRODUCTION

Bring-your-own-device ("BYOD") is an approach to mobile technology that permits access to a company's computer network and email system through employee-owned mobile devices. BYOD permits employees to use the same device for both personal and business purposes. The wide-spread adoption of BYOD programs has been described as "the most radical change to the economics and the culture of client computing in business in decades." More than half of all employees use their personal mobile technology for work.

The BYOD trend has slowly made its way to the legal profession. BYOD has become a viable option for lawyers and law firms for several reasons. First, it theoretically limits a law firm's capital outlays and investment costs as the firm's lawyers purchase the devices on their own. Since no one prefers to carry multiple devices, a BYOD approach to technology permits the consolidation of devices. It provides a convenient option for managing personal and professional information, especially when lawyers are outside the office.

3 Joshua Poje, Security Snapshot: Threats and Opportunities, in ABA TECHREPORT 2013 (2013), available at http://www.americanbar.org/publications/techreport/2013/security_snapshot_threats_and_opportunities.html (reporting that 34% of the respondents to the ABA's 2013 legal technology survey "reported that their firms allowed them to connect their personal mobile devices to the network without restriction") (emphasis in original).
4 At least one study, however, suggests that a BYOD approach will actually result in higher costs. See Tom Kaneshige, BYOD If You Think You're Saving Money, Think Again, CIO, (Apr. 4, 2012, 8:00 AM), http://www.cio.com/article/2397529/consumer-technology/byod--if-you-think-you-re-saving-money--think-again.html (discussing a study by the Aberdeen Group of a company with 1,000 mobile devices which concluded that the company spent "an extra $170,000 per year, on average, when they use a BYOD approach").
Because it allows employees to work with a device or a platform they know and may prefer to use, BYOD evangelists suggest that its adoption improves efficiency. BYOD proponents also claim it gives "employees the freedom to work and collaborate the way they prefer making for a more mobile, productive, and satisfied workforce."\textsuperscript{5} With the development of wearable devices such as smart watches, smart jewelry, and Google Glass, as well as health or fitness sensors that are designed to communicate with apps on a mobile device, they are quickly becoming the center of an individual's personal area network ("PAN").\textsuperscript{6}

The proliferation of mobile devices, however, trigger a number of unique risks for lawyers and law firms, especially in light of our ethical obligation to competently safeguard client information under the Model Rules of Professional Conduct. Superimposed on a lawyer's ethical duty to safeguard client information is the statutory obligation imposed by state and federal laws and regulations to protect various categories of personally identifying information, non-public financial information and protected health information.

Mobile devices permit lawyers and staff to engage in social networking around the clock. One of the hidden risks of social media activity, however, is that the information posted on social media sites by lawyers and staff frequently can provide ample information for cyber criminals to develop sophisticated spear phishing schemes directed at law-firm personnel.

BYOD limits a law firm's ability to control the use of these devices in the same fashion it controls the use of computers and equipment owned and supplied by the firm. In an environment where mobile devices are corporately owned and supplied, a law firm has complete control of the type of devices permitted to access its network, can mandate the use of strong passwords to access the device, ensure the device is locked out after a short period of inactivity or after a certain number of failed attempts to log onto the device, limit how the phone or device can be used, ensure the device is encrypted, lock down the device's browser, limit the user's ability to visit malicious or suspicious websites, provide a whitelist of applications that could be downloaded on the device or a blacklist of applications prohibited on the device, ensure that the latest endpoint security is available and remotely wipe the device if it is lost or stolen. In an

---


unregulated BYOD environment, many of these responsibilities are transferred to the device's owner. As a result, clients in some industries are pushing back against law firm BYOD strategies.7

A mobile device that becomes infected with malware can serve as a launching pad for an attack on the firm's network and potentially place both client and firm information at risk. An unprotected device that is lost or stolen can trigger a reporting obligation if the device contained or provided access to certain categories of unencrypted information.

A law firm's failure to have a comprehensive BYOD policy is a prescription for disaster. An ill-conceived BYOD policy, one that is not disseminated throughout the firm,8 or one that is not routinely enforced, complicates a law firm's ability to safeguard client and firm information.

This article will outline the ethical risks triggered by BYOD and provide suggestions towards developing a comprehensive data security policy for mobile devices that will help mitigate the risks posed by the adoption of a BYOD approach to mobile technology. Part II addresses the impact of technology on the legal profession and discusses how technology has fundamentally altered the delivery of legal services. Part III reviews the lawyer's duty of competence and addresses how that duty includes knowing the risks and benefits of technology and what that ethical duty entails. Part IV outlines the various risks triggered by the adoption of a BYOD approach to mobile technology. Part V addresses a lawyer's ethical duty to safeguard information and communications against technology-based risks and Part VI outlines a law firm's obligation to have measures in place that provide reasonable assurance that its lawyers are conforming to the Rules of Professional Conduct and that the conduct of its non-lawyer assistants is compatible with those professional obligations. Part VI also includes a discussion of ethics opinions addressing cloud computing because mobile devices and the cloud go hand-in-hand. Part VII of this article provides recommendations for law firms adopting a BYOD approach to mobile technology, and concludes with a sample policy addressing data security for mobile devices in Part VIII.


8 Poje, supra note 3 (noting 13% of lawyers responding to the ABA's 2013 legal technology survey did not know "if their firm had any technology polices in place" and noting "the widest knowledge gap is among younger law firm attorneys," including "29% of associates" and "21% of attorneys under the age of 40").
II. THE IMPACT OF TECHNOLOGY ON THE LEGAL PROFESSION

Relentless advances in technology have fundamentally altered the delivery of legal services. Technology provides lawyers the ability to remotely practice from any location, and has cut the tether that traditionally bound lawyers to the bricks and mortar of a law firm. It has made the virtual law office a reality.9

Technology has also altered how we interact and communicate with our clients, third parties and one another. Text messaging and email have relegated written notes and letters to the horse and buggy era. Communications are more immediate and less formal than ever before. Social media has further blurred the line between our personal and professional lives and provides another means to virtually connect with anyone at anytime from anywhere.

At one time, law firms could protect information in their possession the same way kings protected their castle in the Middle Ages – by building a strong perimeter. Rather than a moat with a drawbridge and high stone walls, locks on doors and file cabinets and a clean desk policy provided the necessary protection. When the Internet came into use, a firewall was added to the law firm’s perimeter defenses. Once technology became mobile, however, the perimeter of the "castle's walls" became much harder to defend.

The mobility of modern technology has made protecting client information a far more complex and difficult task for lawyers and law firms than ever before. Innovative communication and file sharing technologies, wireless internet connections, the growing popularity of cloud computing, and the proliferation of mobile devices have significantly complicated the ethical duties and the statutory obligations imposed upon lawyers to protect information entrusted to them.10 “Nearly ubiquitous connectivity disperses nearly ubiquitous vulnerability.”11

---


10 In 1996 Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), which set a federal privacy floor for personally identifying information in health records. Subsequently, in 2009 Congress adopted the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), Pub. L. No. 111-5, Div. A, Title XIII, Div. B, Title IV, 123 Stat. 226, 467 (2009), which among other things, extended the HIPAA obligations of physicians, hospitals, group health plans and other “covered entities” to protect PHI (“protected health information”) to “business associates.” The HITECH Act's final regulations were published in January 2013 as the HIPAA Omnibus Final Rule ("Omnibus Rule"). Business associates were given until September 23, 2013 to comply with the Omnibus Rule. A lawyer or law firm that receives, transmits, uses or maintains PHI in the
The advent of consumer file-sharing technologies like Dropbox, SugarSync, and Beehive, and cloud-based software through which information can be readily transferred outside the firm network has rendered the "castle's" perimeter defenses illusory. Technology provides the means to bypass locked doors and filing cabinets and circumvent traditional methods used to protect confidential information and communications.

Technology also brings hackers to the doorstep of every law firm. In November of 2011, the FBI held a meeting with 200 law firms in New York where it explained that hackers consider law firms to be the "back door to the valuable data of their corporate clients." Mandiant, a cyber-security firm, estimated that in 2011 at least 80 major law firms in the U.S. had been hacked. Hackers and cyber criminals target law firms for two reasons: the perception that law firms' cyber defenses are weaker than that of their clients, and the concentration of valuable information firms accumulate. As a result, the computer networks of law firms are frequently probed for vulnerabilities, and

course of providing legal services to a covered entity or another business associate generally qualifies as a business associate under HIPAA and must comply with its applicable privacy and security requirements.


12 See, e.g., Debra Cassens Weiss, Suit Claims Ex-Partner Installed Software Allowing Continued Access to Law Firm Files, ABA JOURNAL (Feb. 13, 2012, 1:31 PM CST), http://www.abajournal.com/news/article/suit_claims_expartner_installed_software_allowing_continued_access_to_law_/ (addressing a lawsuit brought against a former partner of a law firm who allegedly downloaded Dropbox onto the firm's network to continue accessing files via the Cloud following his departure from the firm).


14 Id.

15 Ed Finkel, Cybersapce Under Siege, ABA JOURNAL (Nov. 1, 2010, 9:58 AM CDT), http://www.abajournal.com/magazine/article/cyberspace_under_siege/ ("Law firms have tremendous concentrations of really critical private information' ... and breaking into a firm's computer system 'is a really optimal way to obtain economic and personal security information.'" (quoting Bradford A. Bleier, unit chief to the Cyber National Security Section in the FBI's Cyber Division)).

16 Matthew Goldstein, Wall St. Is Told to Tighten Digital Security of Partners, N.Y. TIMES, April 8, 2015, http://www.nytimes.com/2015/04/09/business/dealbook/wall-st-is-told-to-tighten-digital-security-of-partners.html?_r=0 (noting "law firms were a logical target for hackers because they are rich repositories for confidential data").
hackers are routinely sending socially engineered emails to lawyers with attachments containing malware or links to malicious web sites.

While hackers’ motives are understood and their attack strategies are known, preventing successful hacks has proven to be difficult. The unfortunate reality is that many successful security breaches could have been avoided if a vulnerability had been timely patched, or if an employee had simply avoided clicking on a link in an email from a person he or she did not know. While data breaches resulting from malicious hackers have grabbed headlines, more data breaches are the result of human error, lost or stolen mobile devices, bad disposal practices and computer glitches than the work of hackers. Confidential information can be compromised simply by misaddressing an email or by clicking "reply to all." While there are technological solutions that can strengthen a law firm’s defenses, frequently the weakest link in the security of a law firm is its personnel.

Further complicating matters is that cyber threats are constantly evolving. Spam filters will capture some phishing emails and anti-virus protection will recognize off-

---


19 The Online Trust Alliance analyzed nearly 500 breaches reported in the first half of 2014 and concluded "upwards of 90% could have been avoided had simple controls and security best practices been implemented." Security and Privacy Enhancing Best Practices, 2015 BEST PRACTICES & CONTROLS (Online Trust Alliance), Jan. 21, 2015, available at https://www.otalliance.org/system/files/files/resource/documents/ota2015-bestpractices.pdf.


the-shelf forms of malware, but hackers are developing new methods to evade those filters and are refining malware to avoid detection. Malware is now designed to specifically target mobile devices. As a result, constant vigilance is required, and security measures must adapt as new threats emerge.

There is no “one size fits all” approach to how law firms protect the information in their possession. Variables such as a law firm’s size, its culture, geographic footprint, office structure, practice areas, technological sophistication and available resources are factors that influence a law firm's approach to protecting the information in its possession.

While ethical discussions involving protecting client information and cyber security frequently focus on available technological tools, even the best technological defenses are no guarantee against a data breach. Rather, a holistic approach to data protection and cyber security is required. Security experts recommend layers of protection or "defense in depth." Because no technological solution is foolproof, coordinated technical, administrative and physical safeguards are needed to protect information. Robust technical, administrative and physical safeguards a law firm puts in place to protect client information, however, can be bypassed by employee carelessness or refusal to follow the firm's security protocols. As a result, any discussion of the duty to protect information should not overlook physical and administrative safeguards to protect information, the education and training of lawyers and staff on the firm's security measures, and consistent discipline if those security measures are violated.

III. A LAWYER'S DUTY OF COMPETENCE REQUIRES KNOWING THE RISKS AND BENEFITS OF TECHNOLOGY

A lawyer's fundamental ethical duty is to provide competent representation to a client. This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary" for the engagement. The Model Rules of Professional Conduct were modified in 2012 to confirm that a lawyer's duty of competence includes knowing

---


23 See, e.g., Cal. State Bar, Formal Op. 2012-184, n.8 (2012) (noting a lawyer, "may employ the most up-to-date security precautions for his server," but would nonetheless violate the obligation to take reasonable precautions to protect client information if he "fail[ed] to lock the door to his office, thereby allowing anyone to come in and rifle through his clients' paper files").

the risks and benefits associated with the technology used by a lawyer in the delivery of legal services. While various state ethics opinions had previously addressed technology issues, the Model Rules had not, and the 2012 amendments to the Model Rules "reflect[ed] technology's growing importance to the delivery of legal and law-related services."

The 2012 amendment to Model Rule 1.1 precludes a lawyer from pleading ignorance of the risks associated with technology. Lawyers are expected to have at least a basic understanding of the risks associated with the technologies they use and the protections available to mitigate those risks. This obviously includes mobile devices used by lawyers.

The obligation to be aware of the "benefits and risks" of relevant technology under Model Rule 1.1 is a nebulous one, but the Chief Reporter of the ABA Commission on Ethics 20/20 explained that the standard had to be because "a competent lawyer's skill set needs to evolve along with technology itself," and "the specific skills lawyers will need in the decades ahead are difficult to imagine." Indeed, the risks to client information and how that information should be protected a decade from now will likely be far different than at present.

While attorneys need not become technology experts or "develop a mastery of the security features and deficiencies" of every available technology:


26 See, e.g., Fla. Bar, Opinion 10-2 (2010) ("A lawyer who chooses to use [d]evices that contain [s]torage [m]edia such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the [d]evice is sanitized before disposition.") That opinion explains the obligation to take reasonable steps includes identifying potential threats to client confidentiality involving those devices, implementing policies to address those threats, inventorining devices that contain hard drives or other storage media, and supervising non-lawyers to obtain adequate assurances that confidentiality will be maintained.


29 Perlman, supra note 27, at 25.
[T]he duties of confidentiality and competence … do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.  

Another proposed state ethics opinion explains that a lack of technical knowledge can render even a highly experienced attorney ethically incompetent to handle a matter "absent curative assistance."  

If an attorney lacks a basic understanding of the risks inherent in the technologies he or she uses to provide legal services, how can the attorney take "reasonable steps" to competently guard against those risks? The duty of competence is the foundation on which the ethical obligation to protect client information rests. As with other skills or practice areas, a lawyer’s duty of technological competence can be achieved through continuing study and education or through association with others who are competent in the area.

The duty of competence also requires that lawyers be aware of the benefits and risks of emerging technologies that can be used to deliver legal services and how advances in existing technologies can impact the security of information in their possession. The difficulty that we face on this issue is the speed at which technology


32 MODEL RULES OF PROF’L CONDUCT R. 1.1 cmts. [2],[8] (2013); Cal. State Bar, Formal Op. 2012-184 (2012) ("If Attorney lacks the necessary competence to assess the security of the technology, she must seek additional information, or consult with someone who possesses the necessary knowledge, such as an information technology consultant."); Iowa State Bar Ass’n, Ethics Op. 11-01 (2011) (noting lawyers can meet due diligence technology requirements "by relying on the … services of independent companies, bar associations or other similar organizations or through its own qualified employees").

is advancing. The mobile phones now carried by many lawyers have more computing power and storage capacity than many desktop computers had a decade ago. When it comes to understanding the risks and benefits of technology, the lawyer's duty of competence must evolve as the technologies we use to provide legal services evolve.\textsuperscript{34}

IV. THE RISKS ASSOCIATED WITH MOBILE DEVICES

Mobile devices present several unique risks, which Model Rule 1.1 requires lawyers to be aware. The nature of mobile devices "places them at higher exposure to threats" than desktop or laptop computers within a law firm's network.\textsuperscript{35}

While laptop computers present the same type of mobility risks as smart phones, tablets and other portable devices, "the security controls available for laptops today are quite different than those available for smart phones, tablets, and other mobile device types."\textsuperscript{36} Additionally, in many instances laptop computers are owned and supplied by law firms. Therefore, they are excluded from the following discussion of BYOD risk. Law firms can and should exercise complete control over the configuration and security of their laptop computers by removing the user's administrative rights over their laptops and firm-supplied technology equipment. Firms should address in their technology policies the use of technical safeguards such as hard drive encryption, locking down the browser, the use of strong passwords, remote wiping, blocking access to blacklisted web sites and other safety measures for their laptop computers.

Flash drives and external hard drives similarly permit lawyers to transport client and firm information with them, and thus, share the same type of portability risk as mobile devices. But portable flash drives and external hard drives lack the computational and WiFi capabilities of mobile devices. Therefore, they are also excluded from the following discussion of BYOD risks. A law firm should nonetheless consider addressing the portability risk of flash drives and external hard drives in its technology policies. Encrypting flash drives and portable external hard drives or other forms of mobile storage should be considered. And because mobile devices can be

\textsuperscript{34} Cal. State Bar, Formal Op. 2012-184 (2012) (noting "[a]s technologies change, ... security standards also may change" and explaining attorneys "should keep abreast of the most current standards so that [they] can evaluate whether the measures taken ... to protect client confidentiality have not become outdated").

\textsuperscript{35} MURUGIAH SOUPAYA & KAREN SCARFONE, NAT'L INST. STANDARDS & TECH., SPEC. PUB. 800-124 REV. 1, GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES IN THE ENTERPRISE 3 (2013).

\textsuperscript{36} Id. at 2.
backed up through the use of an external hard drive or a home computer, limiting or prohibiting the transfer of firm or client information to home computers or external hard drives is another issue to consider in the firm's mobile device policy if it is not covered in another firm technology policy.

**Lost or Stolen Device Risk:** The mobility of smart phones and tablets is what makes them so popular; they allow lawyers to potentially transport confidential client and firm information with them or access that information from any place where they can find an internet connection. Given their size and mobility, however, mobile devices can be easily lost, misplaced or stolen. Information that is either stored on or can be accessed by a mobile device may be compromised when a device is lost or stolen.

Last year, it was estimated that 3.1 million smart phones were stolen in the United States and another 1.4 million phones were lost and never recovered. All too often, these devices are protected by weak passwords, or a four-digit PIN that can be "cracked" by a cyber-criminal's brute force attack on the device. A poorly secured mobile device can result in the loss of confidential client or firm information and trigger another risk stemming from a statutory or ethical obligation to report a security incident or data breach to a client or third parties whose information was placed at risk.

**Data Breach Reporting Risk:** Should a mobile device be lost or stolen, a firm must analyze whether the loss triggers a statutory or ethical reporting obligation. This in turn depends on how the device was protected.

The focus of most state data breach notification laws is the unauthorized acquisition or access to unencrypted computerized data that contains personally identifying information. HIPAA is potentially applicable to law firms that qualify as a


40 Forty-seven (47) states, the District of Columbia, the Virgin Islands, Puerto Rico and Guam have adopted data breach notification laws that potentially apply to data breaches involving lawyers and law firms. See Security Breach Notification Laws, NAT’L CONF. ST. LEG. (Jan. 12, 2015),
business associate. The failure to encrypt a mobile device can trigger a duty to report under one or more of the state data breach laws or HIPAA when an inadequately protected mobile device is lost or stolen. In addition to these statutory reporting obligations involving personally identifying or protected health information, a law firm may also have to evaluate whether an ethical duty to report is triggered under Model Rule 1.4 when other types of client information have been compromised as a result of a lost or stolen mobile device.

Risk That Some Devices Should Not Be Trusted: While the configuration of smart phones includes basic built-in restrictions or architecture, those security restrictions can be easily compromised by a user in order to download software or third-party applications that would not normally be permitted by the device. This is referred to as jailbreaking (iOS, Apple's operating system) or rooting (Android) a phone, which will provide the user with escalated privileges or root access to the device. Jailbreaking or rooting a smartphone renders it more vulnerable to a malicious attack and should not be permitted in a BYOD environment.41

Some mobile devices are built on platforms that may have vulnerabilities that can be exploited. For instance, it was recently discovered that nearly half of all Android devices are vulnerable "to a newly discovered hack" that allows "attackers to surreptitiously modify or replace seemingly benign apps with malicious ones that steal passwords and other sensitive data."42

Additionally, unless the firm's network has a device directory that recognizes mobile devices that are permitted access, nothing prevents an attorney from using a family member's tablet or smart phone, and gaining access to the firm's network through his or her log-in and password credentials. In this scenario, the lawyer can download client information to the device which will place it completely outside the firm's network and on a device that may lack the protection required by the firm's mobile device policy. This risk can be addressed through technical network or MDM controls that limit access to only mobile devices recognized by the system or data loss

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Currently, only Alabama, New Mexico and South Dakota have not enacted a data breach notification law. Id.


prevention tools that will block the downloading of information to an unrecognized device and through the firm's mobile device policy that prohibits this type of activity.

Cloud Computing and Shadow IT Risk: Owners of BYOD devices frequently will download software they prefer to use when working remotely and applications for their personal use during off hours. Thus, BYOD inevitably brings with it BYOS ("Bring Your Own Software") and BYOA ("Bring Your Own Applications") because of their popularity and ease of use. Frequently, this software is cloud based, which means BYOD often also frequently results in BYOC ("Bring Your Own Cloud"). Technology security experts refer to this as the rise of "Shadow IT."43 BYOS, BYOA and BYOC raise additional ethical issues and risks for law firms and their lawyers described below that should be addressed in a firm's technology policies and BYOD policy.

Insecure Network Risk: Public WiFi is convenient and easy to use when outside the office, but using it is rife with security risks. When a lawyer connects to public WiFi without the need for a password, the attorney is using an unencrypted connection to an insecure network. The lawyer is vulnerable to eavesdropping and "man-in-the-middle" ("MTM") attacks in this context. A MTM attack redirects a victim's email to the hacker's device, which allows the hacker to compromise the victim's mobile device and can provide the attacker "with access to the corporate network."44 This risk is one that can be addressed in training sessions and law firm technology policies. Lawyers should be advised to avoid using Public WiFi to work on client documents or to email client or firm information and to turn off any feature on their device that allows it to automatically connect to nearby available networks.

It is unrealistic, however, for a law firm to expect its lawyers will never use an insecure Wi-Fi network when outside the office. Firms should therefore attempt to offer reasonable alternatives for their lawyers that will mitigate this risk. The key to limiting this risk is to provide an encrypted and secure link for communicating and connecting with the firm's network, such as through the use of Citrix or VPN. Law firms should also consider some form of dual factor authentication for remote access to the firm's network.

43 Shadow IT refers to IT "solutions used within an [organization] without the approval, or even the knowledge, of corporate IT." It is also "often referred to as the [consumerization] of IT." Vawns Guest & Patrick Bolger, Managing Shadow IT, COMPUTERWEEKLY, http://www.computerweekly.com/opinion/Managing-shadow-IT (last visited Apr. 7, 2015).

Ediscovery/Spoliation Risk: A duty to preserve potentially relevant information is triggered when litigation is reasonably anticipated. When a law firm is sued or threatened with a lawsuit, it must preserve electronically stored information ("ESI") in its possession, custody or under its control. This can include ESI stored on attorney or employee-owned mobile devices. Additionally, information on a mobile device may have to be produced in response to a subpoena or reviewed in connection with a government regulation. A law firm's failure to preserve ESI on its lawyer's mobile devices can potentially trigger a spoliation claim. 45

While emails sent or received from a mobile device that is linked to a law firm's email system should be stored on the firm's email server once the device is properly configured and synchronized, text messages and emails sent via a personal, web-based email account on the device will not reside on the firm's servers. And documents potentially can be moved to a Cloud, to a home computer or to a personal storage device from a mobile device. In formulating a litigation hold, law firms should not overlook their employees' mobile devices, home computers and personal storage devices where potentially relevant ESI may be located. It should be anticipated that lawyers will want to protect their personal privacy and limit access to their home computers and personal devices. This can be accomplished by them not transferring work-related ESI to home computers or backing up their devices to home computers or personal storage devices. To limit this clash of interests and to limit the risk of spoliation, a law firm should consider addressing these issues in either its technology policies or specifically in its BYOD policy.

Privacy Risk: In Riley v. California, the Supreme Court recognized that the owner of a cell phone has a reasonable expectation of privacy in the digital content stored on the phone for purposes of the Fourth Amendment. 46 While the Fourth Amendment is inapplicable to law firms, the Electronic Communications Privacy Act ("ECPA") does apply. The ECPA was intended to protect against privacy intrusions not encompassed by the Fourth Amendment.47

45 See, e.g., Southeastern Mechanical Servs., Inc. v. Brody, 657 F. Supp.2d 1293 (M.D. Fla. 2009) (awarding spoliation sanctions, in the form of an adverse inference instruction, for failing to properly preserve ESI on BlackBerries). In Southeastern Mechanical, BlackBerries were wiped which resulted in the loss of emails before the smart phones were synchronized with the company's email server, as well as the loss of text messages and call logs that would only reside on the device and not the company's servers.

46 134 S.Ct. 2473 (2014) (rejecting the search incident to arrest exception to the Fourth Amendment's warrant requirement).

47 Garcia v. City of Laredo, Tex., 702 F.3d 788, 791 (5th Cir. 2012).
The ECPA protects the privacy of electronic communications, but recognizes an exception that allows the access or interception of electronic communications where consent is provided. The Computer Fraud and Abuse Act ("CFAA") similarly prohibits the unauthorized access to a computer and provides a civil remedy when the damages resulting from that access exceed $5,000.

Law firms generally have a policy on the use of the firm's equipment, computers, email system and network, which explains that the firm monitors the use of these resources and provides that a user should have no expectation of privacy in their use. Some firms may have similar statements on electronic banners that appear whenever a person logs onto the firm's network. These statements may provide that by logging on to the system, accessing the firm's network, or by using its equipment, the user consents to the firm's monitoring the use of the firm's equipment and systems, as well as the firm's review of any documents created or any electronic communications sent or received over its network or via its systems. Similar statements should be included in the firm's BYOD policy to avoid a claim that the ECPA or the CFAA were violated by the firm monitoring work-related emails sent from a personally-owned mobile device.

While these "no expectation of privacy" policies have been generally upheld, one state Supreme Court has ruled to the contrary. In Stengart v. Loving Care Agency, Inc., the New Jersey Supreme Court addressed whether an employer could review emails sent on a company-issued laptop through a personal, password-protected, web-based (Yahoo) email account. The court in Stengart concluded the emails were privileged and observed: "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." While other states have not

53 Id. at 665. The court in also noted, however: "Our conclusion that Stengart had an expectation of privacy in e-mails with her lawyer does not mean that employers cannot monitor or regulate the use of workplace computers. Companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy."
followed *Stengart's* approach, some courts still recognize a privacy distinction between personal and business email accounts and may also consider an employee's efforts to protect documents or emails from review and disclosure even though they are sent from a company computer.

The Stored Communications Act ("SCA") further prohibits the unauthorized access to stored communications, such as email, held by a service provider. The SCA also can be violated when a party “intentionally exceeds” its authorization to gain access to an electronic communication “while it is in electronic storage.” When firm or client information is stored in the Cloud by an attorney, the law firm will need the lawyer's permission to delete or remove it from the Cloud to avoid running afoul of the SCA. Firms should consider including an employee consent provision in their mobile device policy which authorizes the firm to remove any client or firm information from a non-approved Cloud that was moved to the Cloud by one of its attorneys.

Should it become necessary to wipe a lost or stolen mobile device, the firm should obtain the lawyer or employee's written permission to avoid a claim under the Computer Fraud and Abuse Act. Both personal and work related information will likely be deleted when the device is wiped. That factor should be spelled out in the law firm's BYOD policy to avoid a claim that the owner of the device did not know the personal


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

56 See, e.g., *Rajae v. Design Tech Homes, Ltd.*, Civil Action No. H-13-2517, 2014 WL 5878477, at *3-4 (S.D.Tex. Nov. 11, 2014) (ruling the CFAA was not violated because plaintiff failed to establish that his damages met the Act’s $5,000 threshold following the deletion of personal information on plaintiff's personally owned mobile device by his former employer).

57 See, e.g., *People v. Jiang*, 33 Cal. Rptr. 184 (Cal. Ct. App. 2005) (holding an employee's emails to his attorney were privileged notwithstanding they were sent via his employer's computer in light of the employee's "substantive efforts to protect the documents from disclosure by password-protecting them and segregating them in a clearly marked and designated folder"). The court in *Jiang*, however, also noted that the employer's electronic communications policy did not specifically prohibit the employee's personal use of the company's computer system.


59 *Id. at § 2701(a)(2).*
information would be deleted when the device was wiped and that had he or she known, would not have allowed the device to be wiped.60

**Malware Risk:** Malware targeting mobile devices has risen significantly and is becoming more complex.61 Depending on the configuration of a law firm's network, these devices may lack the same endpoint security that is available within the firm's firewall for its desktop or laptop computers.62 Antivirus and anti-malware tools require frequent updates to remain effective, which may not be a priority for the device's owner. A compromised smart phone or tablet, however, can serve as a launching pad for malware to steal information from the lawyer who owns the device and to gain a foothold in the law firm's network.

**Untrusted Applications Risk:** Because a BYOD device is personally owned, a law firm loses control over what applications are downloaded on the device, or what steps the owner takes while downloading any application on the device.63 Many seemingly harmless applications contain security vulnerabilities or malicious payloads that can readily compromise the device.64 A report from Webroot revealed that 42% of

---


62 Craig Sprosts, *Companies Weigh BYOD vs. COPE, But What Really Protects Data?*, WIRED, http://www.wired.com/2013/05/companies-weigh-byod-vs-cope-but-what-really-protects-data/ (noting "although there is a litany of anti-virus applications available on the iPhone App Store and in the Android Marketplace, these applications detect a fraction of threats and can be disabled by malware that gains administrative access to the device") (last visited Apr. 8, 2015).

63 TREND MICRO, *supra* note 61 ("Malware creators are banking on the average user's lack of awareness when it comes to properly setting mobile devices and downloading apps from known safe, legitimate services.").

64 Yulong Zhang, Hui Xue, Tao Wei & Zhaofeng Chen, *Freak Out on Mobile*, FIREEYE BLOG (Mar. 17, 2015), https://www.fireeye.com/blog/threat-research/2015/03/freak_out_on_mobile.html ("After scanning 10,985 popular Google Play Android apps with more than 1 million downloads each, we found 1228 (11.2%) of them are vulnerable to a FREAK attack because they use a vulnerable OpenSSL library to connect to vulnerable HTTPS servers. These 1228 apps have been downloaded over 6.3 billion times. Of these 1228 Android apps, 664 use Android’s bundled OpenSSL library and 564 have their own compiled OpenSSL library. All these Open SSL versions are vulnerable to FREAK. On the iOS side [Apple iPhones], 771 out of 14,079 (5.5%) popular iOS apps connect to vulnerable HTTPS servers. These apps are vulnerable to FREAK attacks on iOS versions lower than 8.2. Seven [sic] these 771 apps have their own vulnerable versions of OpenSSL and they remain vulnerable on iOS 8.2.")
all Android apps they tested between 2011 and 2013 were classified as malicious, unwanted or suspicious. With personally owned devices, a firm may also lose the ability to block the user from visiting suspicious websites or URLs that deliver some form of malware to their visitors.

**Unauthorized User Risk:** Another risk involves the unauthorized use of a mobile device by friends, acquaintances and family members that may have access to the device. It is not unusual for a mobile device to be left unattended at home. Applications can be downloaded on the device by family members, and confidential personal information or client information can be accessed if use of the device is not carefully monitored and controlled, even at home.

**Risk of Inappropriate Use:** While law firms may not be able to control how their attorneys use a personally owned mobile device, firms should consider adopting policies and providing training that may help to mitigate that risk. Certain web sites may download malware onto a mobile device when the lawyer visits such a site while surfing the net. This is referred to as a "drive-by-download of malware." Lawyers should be alerted to this risk and to avoid visiting music, video and adult web sites because of this risk. Another hacker trick is to add a malicious payload into advertisements appearing on sites that appear to be harmless and are frequently visited. When someone clicks on the ad, the payload is launched. Lawyers and staff should be alerted to this risk as well and be advised that they can reduce this risk by either disabling the Java plug-in in the device’s browser or updating the plug-in to its latest version. And as explained below, a robust MDM application can be potentially

__________________________


66 Java is a programming language that works across multiple computing platforms and is routinely found in plug-ins in web browsers. Java has a history of vulnerabilities. According to Kaspersky Lab, Java was responsible for fifty percent of all cyber-attacks in 2012. See “Oracle Java surpasses Adobe Reader as the most frequently exploited software,” KASPERSKY LAB (Dec. 21, 2012), http://www.kaspersky.com/about/news/virus/2012/Oracle_Java_surpasses_Adobe_Reader_as_the_most_frequently_exploited_software. Symantec has also indicated that hackers continue to “exploit Java vulnerabilities where users have not upgraded to newer, more secure Java versions.” SYMANTEC CORP., INTERNET SECURITY THREAT REPORT 59 (2014), available at http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf.
configured to block access to various web sites and URLs using publicly available blocklists or reputation services.

The risk of distracted driving is well known, and lawyers who attempt to review or send email or text messages while driving place themselves and others at risk. A firm should consider prohibiting the use of a mobile device to review or send email or text messages while driving in either its technology policies or in its mobile device policy. Additionally, law firms should be aware of a recent appellate decision from New Jersey, Kubert v. Best, which suggested that a person who sends an email or text message to someone he or she knows is driving a vehicle could be held liable if the driver is involved in an accident while reviewing the message. In light of Kubert, law firms may want to consider whether it should prohibit sending email or text messages to someone its lawyers or staff know or have reason to know is operating a motor vehicle.

A firm should also clearly provide that its policies prohibiting harassment and discrimination apply to any inappropriate email, text message, blog or social media post sent via mobile device linked to the firm's network. Merely because an inappropriate message or post was sent outside the office during an off-hour will not insulate the firm from potential liability. This is especially true where the firm has advised its employees that they have no expectation of privacy in the use of the firm's network, or systems, and reserves the right to review any emails or communications via devices linked to its network.

**Geo Location Risk:** Mobile devices frequently come equipped with global positioning technology which allows a device to map a location and identify nearby business. These "location services" are frequently used in social media activities and by various applications download on the device which commonly share the user's location with retailers and merchants. Besides compromising the user's personal privacy, location services increase the "risk of targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are, and to correlate that information with other sources" such as "who the user associates with and the kinds of activities they perform in particular locations."68

**Voice to Text Risk:** Many smart phones also have a voice-to-text feature that allows the user to dictate email or text messages sent via the device. While this feature is easy, convenient and more efficient than using your thumbs to type the message, the

---


68 SOUPAYA & SCARFONNE, supra note 35 at 6.
information dictated to your phone is recorded by the device and sent to third parties for review for quality control purposes.\textsuperscript{69}

**MDM Risks:** Mobile device management (MDM) solutions are available that will segregate personal and firm information on the device, provide a secure connection to a law firm’s network and email system, and can help control some of the risks associated with a BYOD approach to mobile technology. MDM applications can be used to enforce strong passwords, lock the device after a specified number of unsuccessful log-ins or after a period of inactivity, encrypt the device and provide the ability to remotely wipe a lost or stolen mobile device. Some MDM solutions can identify smart phones that have been rooted or jailbroken, and have features that can help secure the device’s browser. MDM tools, however, also have vulnerabilities that can be compromised by hackers. Some of these vulnerabilities "include ignoring authentication, sending login tokens without encryption (and in some cases, configuring those tokens to never expire), which could allow an attacker "to wipe innocent phones" or to "access everything the legit [phone] can: email, shared drives, documents, etc."\textsuperscript{70}

There are multiple MDM options available to law firms. These include third-party applications that can be downloaded onto a device in addition to the MDM capabilities that are built into many devices. When deciding which MDM option to deploy the security of these options themselves is a factor to consider, in addition to the types of controls available through each option.

**Wage and Hour/Expense Reimbursement Risk:** Although attorneys are generally considered exempt employees for purposes of wage and hour claims, most law firm employees or staff and paralegals are not exempt and have a right to claim overtime for their off-the-clock work. The Fair Labor Standards Act ("FLSA") mandates that nonexempt employees be paid for work that they are "permitted" to perform.\textsuperscript{71} Additionally, if a law firm "knows or has reason to believe" that work is being performed by nonexempt employees, then it "must count the time as hours worked."\textsuperscript{72} Thus, answering emails or working via mobile devices by nonexempt employees of a


\textsuperscript{71} 29 U.S.C. §§203(g) (2014), 207(a) (2010); 29 C.F.R. § 785.11 (2013) ("Work not requested but suffered or permitted to perform is work time.").

\textsuperscript{72} 29 C.F.R. §785.12 (2013).
A law firm can potentially trigger a wage and hour claim by those employees unless they are told to keep track of their time and compensation.

Therefore, a law firm should evaluate whether any of its nonexempt employees should be granted access to the firm's network or email system under its BYOD policy. The safest approach to limit or avoid this risk is to exclude nonexempt employees from a firm's BYOD policy and not allow them access to the firm's network or their work-related emails outside of their normal working hours. Should a law firm allow nonexempt employees to access its network or email system under a BYOD policy, to limit this risk the firm should clearly prohibit in writing the use of mobile devices by nonexempt employees for any business-related purpose outside of normal working hours. Firms taking this approach should ensure that nonexempt employees are properly informed about this type of limitation and firms should be prepared to consistently enforce and discipline its violation. Further, lawyers and other supervising nonexempt employees should be aware of this policy and the consequences of not adhering to it.

A related BYOD issue is whether an employee is entitled to reimbursement of some or all of the costs of using a personally owned mobile device. The FLSA prohibits an employer from requiring an employee to pay expenses necessary for the performance of the employee's work when the cost of those expenses "cuts into the minimum or overtime wages required to be paid" under the Act.73

This issue was highlighted by the recent decision in Cochran v. Schwan's Home Service, where the California Court of Appeals ruled that under section 2802 of the California Labor Code, an employer is obligated to reimburse an employee "for the reasonable expense of the mandatory use of a personal cell phone."74 The decision in Cochran was not limited to nonexempt employees. So in California, law firms that do not pay or reimburse an employee's cell phone expense under its BYOD policy are at risk for this type of reimbursement claim.75

73  29 C.F.R. §531.35 (2013).
74  Cochran v. Schwan's Home Serv., Inc., 176 Cal. Rptr. 3d 407, 412 (Cal. Ct. App. 2014) ("Otherwise, the employer would receive a windfall because it would be passing its operating expenses onto the employee.").
75  States that have addressed this issue are not uniform in their approach. Several states have laws similar to California that require employers to reimburse all expenditures necessary or required to perform the employee's work. Other states, however, do not require reimbursement for equipment that may be used for both personal and work related purposes. Still other states follow the FLSA approach and only require reimbursement when the expense would reduce the employee's earnings below minimum wage. So this is a risk that is state specific in nature.
Social Media Risk: Because social media networks such as Facebook, LinkedIn, Twitter, YouTube, Instagram or Snapchat are frequently accessed through mobile devices, any discussion of BYOD risks should include a brief mention of social media risks. Social media users frequently discuss various aspects of their professional and personal lives with their friends and followers in posts or tweets on these networks. One obvious risk is that confidential client or firm information may be inappropriately disclosed in a social media post. Model Rule 1.6 not only encompasses any information relating to the representation of a client, but also extends to disclosures "that do not themselves reveal protected information, but could reasonably lead to the discovery of such information by a third person." 76

A less obvious social media risk to client information is the role that it plays in spear phishing exploits of hackers and cyber criminals. 77 Hackers scan social media sites looking for information about a target that can be exploited, such as a list of friends, photos or posts about a person's recent activities. Cyber criminals hope that because a phishing email appears to be from someone the intended target knows or recognizes, they will be less careful in handling the email and either click on a link or an attachment containing malware, or provide information in response to the email that they would not otherwise provide to a stranger.

There is no magic bullet to defeat these exploits. The best way to prevent a successful spear phishing attack is through ongoing training to all lawyers and staff about how to identify phishing emails and social engineering tricks coupled with frequent reminders to never click on attachments or links in suspicious emails or in emails from someone they don't know or emails they were not expecting to receive.

V. THE ETHICAL DUTY TO SAFEGUARD AGAINST TECHNOLOGY-BASED RISKS

If the foundation of a lawyer's ethical duty to safeguard client information is found in Rule 1.1, then Model Rules 1.6 and 1.15 provide the ethical "firewall" that protects client and firm information from the "barbarians" who are seeking access at the "castle's gates."

Model Rule 1.15 requires a lawyer to "hold property of clients or third persons" in the lawyer's possession "separate from the lawyer's own property," and mandates

77 Spear phishing involves a phony or spoofed email that appears to be from a person, company or organization that the intended target knows. Successful spear phishing exploits rely on familiarity with the intended target.
that it be "appropriately safeguarded." Comment 1 to Rule 1.15 explains, "[a] lawyer should hold property of others with the care required of a professional fiduciary." Rule 1.15 applies to property of clients and third persons irrespective of its format; it applies with equal force to tangible property, paper records and electronic information. Comment 1 to Model Rule 1.15 explains it also applies to property received from "prospective" clients.

As it pertains to data security, Rule 1.6 states that a lawyer "shall not reveal" any information "relating to the representation of a client unless the client gives informed consent, [or] the disclosure is impliedly authorized . . . to carry out the representation." Rule 1.6 is not limited to information protected by the attorney-client privilege but "to all information relating to the representation, whatever its source." It extends to disclosures "that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person.

Lawyers are obligated to take "reasonable measures" to safeguard "the integrity and security" of their electronic files. Among other things, this obligation requires that lawyers take "reasonable steps" to ensure that "only authorized individuals have access to the electronic files" and to ensure they "are secure from outside intrusion." Rule 1.6(c) requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Comment 18 lists a series of factors to consider in assessing whether “reasonable efforts” were taken to protect against an inadvertent or unauthorized disclosure or access of information, including:

78 MODEL RULES OF PROF'L CONDUCT R. 1.15(a) (2013).
80 See, e.g., Pa. Bar Ass'n, Formal Op. 2011-200 (2011) ("Client property generally includes files, information and documents, including those existing electronically.").
82 MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2013).
86 Id. (explaining such steps include the use of firewalls, intrusion detection software and backups of all electronically stored files).
87 MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2013).
• The sensitivity of the information.
• The likelihood of disclosure if additional safeguards are not taken.
• The cost of employing additional safeguards.
• The difficulty of implementing the safeguards.
• The extent to which the safeguards adversely affect a lawyer’s ability to represent a client.
• Whether the client required special security measures be taken or provided informed consent to forego security measures that might be required under this rule.88

Thus, Rule 1.6 contemplates a balancing approach when evaluating the security measures that can or should be taken when protecting client information. Various state ethics opinions take a similar approach to the issue.89 Those opinions recognize that "facts and circumstances" can dictate the types of "reasonable protective measures" a lawyer must take to protect information in the lawyer's possession.90 The level of protection may depend on the "type and sensitivity of client information."91 As one ethics opinion explained:

The greater the sensitivity of the information, the less risk an attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent.92

89 See, e.g., Cal. State Bar, Formal Op. 2010-179 (2010) (outlining various factors to consider including "the degree of sensitivity of the information").
90 Id.; Iowa State Bar Ass'n, Ethics Op. 11-01 (2011).
91 N. H. Bar Ass'n, Advisory Op. 2012-13/4 (2013) (addressing cloud computing); see also Iowa State Bar Ass'n, Ethics Op. 11-01 (2011) (recognizing "the degree of protection to be afforded client information varies with the client, matter and information involved").
92 Cal. State Bar, Formal Op. 2010-179 (2010); see also Fla. Bar, Op. 12-3 (2013) (addressing cloud issues involving "particularly sensitive information" and noting a "lawyer should consider whether [to] use the outside service provider or use additional security in [these] specific matters").
These opinions suggest that lawyers and law firms should identify various types of “highly” sensitive information in their possession.

While ethics opinions explain that additional precautions should be considered in various contexts when "highly" or "particularly" sensitive information are involved, they generally do not define or discuss the types of client information that would be encompassed by that rubric. It seems logical, however, for law firms to consider addressing the sensitivity of client information at the outset of any engagement.

This can be accomplished in several ways. The client can be asked if the engagement will involve any highly sensitive information or information warranting special security measures. Additionally, the file intake process can be set up to identify any categories of information that state or federal law treat as highly sensitive in nature or that the firm believes should be treated as highly sensitive. Examples could include personally identifying information, protected health information, non-public financial information, proprietary information, source code, patents, trademarks, trade dress, trade secrets, a merger and acquisition or a high stake business deal. A firm can then take any steps it deems necessary and appropriate to protect that information, including limiting who is permitted to access that information and how it may be transmitted.

Rule 1.6 recognizes that additional safeguards may be required with highly sensitive information, while also noting the cost and difficulty of implementing or using certain types of safeguards are relevant considerations when evaluating whether to apply additional safeguards. The additional safeguards, however, do not have to be technology based. They can, and should, include security awareness training and the development of firm policies involving the use of technology by a firm's lawyers and staff.

The ethical duty to take reasonable precautions clearly does not require measures that will "guarantee" against unauthorized access. Rule 1.6's duty of confidentiality “does not require that a lawyer use only infallibly secure methods” to store and transmit information.


Various ethics opinions have referenced a number of technological options available to protect client information.\footnote{Ariz. State Bar, Ethics Op. 09-04 (2009) ("In satisfying the duty to take reasonable security precautions, lawyers should consider firewalls, password protection schemes, encryption, anti-virus measures, etc.").} Given the speed at which technology is evolving, state ethics opinions generally avoid recommending any particular security measure for fear it will be quickly outmoded.\footnote{See, e.g., Iowa State Bar Ass'n, Ethics Op. 11-01 (2011) ("It is beyond the Committee's ability to conduct a detailed information technology analysis .... Even if we had that ability our analysis would soon be outdated.").} Therefore, state ethics opinions generally leave it to the "sound professional judgment" of the attorney to determine what type of security measures should be taken.\footnote{Ariz. State Bar, Ethics Op. 05-04 (2005) ("Precisely which of these software and hardware systems should be chosen – and the extent to which they must be employed – is beyond the scope and competence of the Committee. This is the kind of thing each attorney must assess."); N. J. Sup. Ct., Op. 701 (2006) (explaining a lawyer "is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access"); Mass. Bar Ass'n, Ethics Op. 12-03 (2012) ("Ultimately, the question of whether the use of Google docs, or any other Internet based data storage service provider, is compatible with [a] Lawyer's ethical obligation to protect his clients' confidential information is one that Lawyer must answer for himself based on the criteria set forth in this opinion.....").}

Comment 18 to Rule 1.6 further notes that whether additional steps are required to comply with other laws such as state and federal laws governing data privacy is beyond the scope of the Rule.\footnote{MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt [18] (2013).} However, HIPAA's Security Rule applies to lawyers and firms that qualify as "business associates" and imposes various physical, administrative and technical safeguards designed to ensure the confidentiality, integrity and access to electronic personal health information.\footnote{See 45 C.F.R. §§ 160.101-160.552, 164.102-164.106, 164.302-164.318 (2014).}

Law firms should not overlook training on data security and the development of policies as important data security measures in accordance with Rule 1.6. If there is one truism when it comes to data security, it is that no technological safeguard is foolproof or can entirely eliminate the risk of unauthorized access to client data. Law firms can have advanced technological safeguards built into their email and information systems, but if lawyers do not know how to use the firm's technology, then those safeguards are rendered worthless. As a result, technology and data security training is an important component to any risk management program for law firms.
An attorney’s duty of confidentiality and the corresponding duty to take appropriate measures or reasonable steps to protect information in a lawyer's possession do not require an attorney-client relationship to exist before it is triggered, as the duty of confidentiality applies once information is received from "prospective" clients.100 Also, Rule 1.6's duty of confidentiality does not end upon the termination of the attorney-client relationship.101 Rule 1.9(c) extends the duty of confidentiality to "former clients" and provides: "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client . . . shall not thereafter . . . (2) reveal information relating to the representation except as these Rules would permit or require with respect to a client."102

Options to protect information stored on a mobile device and comply with the duty of confidentiality could include:

- Protecting it with a strong password.
- Encrypting the device.
- Installing and frequently updating antivirus/anti-malware protection on device;
- Investigating the reputation and reviews of any application before downloading the application on the device,
- Refusing to open attachments or click on links or photographs in any email from an unknown person or in a suspicious looking email you were not expecting to receive;
- Avoiding clicking on advertisements when visiting websites and avoiding websites that have been publicly blacklisted by reputation services;
- Training lawyers and staff on risks and best practices for mobile device use and security.
- Employing a combination of some or all of the above steps.

---

100 See MODEL RULES OF PROF'L CONDUCT R. 1.18(b) (2013) (addressing information received from "prospective" clients and explaining "[e]ven when no client-lawyer relationship ensues, a lawyer … shall not use or reveal that information, except as Rule 1.9 would permit").


102 MODEL RULES OF PROF'L CONDUCT R. 1.9(c) (2013).
The types of physical, administrative and technical safeguards a firm may want to consider when adopting a BYOD approach to mobile technology to safeguard client and Firm information are outlined below in Part VI.

VI. DUTY TO HAVE MEASURES REASONABLY ASSURING THAT LAWYERS ARE CONFORMING TO PROFESSIONAL CONDUCT RULES AND THE CONDUCT OF NON-LAWYER ASSISTANTS IS COMPATIBLE WITH LAWYERS PROFESSIONAL OBLIGATIONS

Most lawyers do not have an IT background or training in computer or network security. That means that law firms must rely on the assistance of IT professionals to create a network infrastructure that will allow its lawyers to work remotely and communicate electronically. This reality triggers the application of Rules 5.1 and 5.3 of the Model Rules of Professional Conduct.

Rule 5.1 imposes supervisory obligations on partners or lawyers with "comparable managerial authority" to ensure the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. This requires "reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance" that the firm's lawyers will conform to the Rules of Professional Conduct including the duty of competence in Rule 1.1 and the duty of confidentiality in Rule 1.6.

Some lawyers value convenience over security and may deliberately work around a firm’s security measures because they either fail to appreciate the risk of their conduct or simply do not care. A law firm’s most tech-savvy lawyers, its Millennials, are the ones most likely to try to circumvent its security rules. While training can help explain the risk to client data, a law firm should consider data security policies that prohibit risky conduct. A law firm must consistently enforce its data security policies and practices in order for them to be effective. This is especially true with personally owned mobile devices.

The development of policies and practices addressing data security, the appropriate use of firm equipment, maintaining the confidentiality of client information, safe internet practices, and associated training on these topics are examples of efforts that can provide "reasonable assurance" that the firm's lawyers are complying with their ethical duties involving data security. Part VI of this article contains

103 MODEL RULES OF PROF'L CONDUCT R. 5.1(a) (2013).


recommendations for Firms to consider when developing a BYOD policy relating to mobile device technology. Whether additional measures beyond "internal policies and procedures" are required will depend on the firm's size and structure, the experience of its lawyers, the nature of its practice and the frequency with which difficult ethical issues arise.\textsuperscript{106}

Rule 5.3 takes an identical approach with non-lawyers who are employed, retained or associated with a lawyer or firm. It requires partners and any lawyer or group of lawyers with "comparable managerial authority" to ensure that the firm has in effect measures giving reasonable assurance that the conduct of non-lawyer assistance "is compatible with the professional obligations of the lawyer."\textsuperscript{107} This means that non-lawyers who work within the firm (e.g., secretaries, IT specialists, docket clerks, paralegals) and those who work outside the firm (e.g., court reporters, IT consultants, expert witnesses, ediscovery vendors) should understand the need to preserve the confidentiality of client and firm information to which they have access.

Comment [2] to Model Rule 5.3 explains that non-lawyer assistants must be given "appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product."\textsuperscript{108} The same is true for non-lawyer assistants who work outside the firm. The extent of this obligation turns on several factors including: the education, experience and reputation of the non-lawyer assistant; the nature of the services provided by the assistant; the terms of any arrangements relating to the protection of client information; as well as the "legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality."\textsuperscript{109} Law firms should not overlook training for its employees and staff on data and cyber security and the confidentiality obligations imposed on the firm and its lawyers.

A. Cloud Computing and Cloud Storage Ethical Issues Arising From Mobile Technology

The term cloud computing refers to the shared use of applications, computing services, and physical or virtual resources over the internet.\textsuperscript{110} Examples of cloud computing applications (BYOA or BYOS) available to lawyers and law firms include

\begin{itemize}
  \item \textsuperscript{106} See MODEL RULES OF PROF'L CONDUCT R. 5.1 cmt. [3] (2013).
  \item \textsuperscript{107} MODEL RULES OF PROF'L CONDUCT R. 5.3(a) (2013).
  \item \textsuperscript{108} MODEL RULES OF PROF'L CONDUCT R. 5.1 cmt. [2] (2013).
  \item \textsuperscript{109} MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [3] (2013).
\end{itemize}
Google Docs, Carbonite, SugarSync, Dropbox and Microsoft Office 365. Documents generated or shared through web-based applications like these are generally stored in the "cloud." Web or internet based email systems such as Gmail and Yahoo also store email and attachments in the "cloud."

Cloud storage refers to an internet-based model of remote data storage on servers typically owned by third parties that host the data, generally at off-site locations.¹¹¹ Cloud storage is simply today's version of a warehouse for electronic records. References to the "cloud" are merely "a fancy way of saying stuff's not on your computer."¹¹²

There are three basic delivery models for cloud computing services. Software as a service (SaaS) is the name of a model though which applications are made available to a user through an interface with the user's computer. Platform as a service (PaaS) is a model used primarily to develop those applications. Infrastructure as a service (IaaS) typically involves a third party host that provides computing resources, such as hardware, servers, storage and other components of a network's infrastructure. Lawyers and law firms would be generally involved with SaaS and IaaS cloud delivery models.

Cloud computing resources are made available or deployed in one of four ways:

- Public clouds which are available for use over a public network by anyone;
- Private clouds which are available for use solely by the employee of a single organization;
- Community clouds which are available to organizations or entities within the same or related service industries or community; or
- Hybrid clouds, which can involve a combination of a public cloud provider with a private cloud platform to perform distinct functions for a single organization. A hybrid cloud provides an organization the flexibility to store information in a private cloud while relying on applications and other computing resources from a public cloud to create or transmit information.

Cloud applications and cloud-based storage typically go hand-in-hand with today's mobile devices by virtue of applications and web-based email accounts on those devices. Cloud-based applications and mobile technology permit lawyers greater flexibility in how they can access and share documents, information or work. Documents or emails can be accessed wherever, whenever and however network or WiFi access can be obtained. Cloud applications and storage can provide significant cost savings to lawyers and firms by eliminating the need to purchase, maintain, upgrade and patch hardware, servers and software applications on an on-going basis; to employ staff to perform those functions; or to rent space to house that equipment. And the security measures that reputable, certified cloud storage providers have in place likely exceed the security of most law firms.  

The use of the cloud, however, implicates the lawyer’s duty of competence under Rule 1.1. Because use of the cloud means that client information will be stored on a third party’s servers, it poses a different set of security risks, as third parties may be permitted to have some form of access to client information. A lawyer's duty to safeguard information under its control cannot be transferred or delegated to a third party, nor is it lessened simply because the lawyer stores client information with a cloud provider. Thus, mobile technology's use of the cloud also triggers consideration of Model Rules 1.6, 1.15, 5.1 and 5.3. Yet how many lawyers have considered whether their use of cloud-based applications or web-based mail accounts on their mobile devices trigger these issues? And how many lawyers have checked Google’s terms of service for instance, and evaluated the potential impact of those service terms on the duty to maintain the confidentiality and security of client information?

---

113 See, e.g., N.J. Sup. Ct. Op., 701 (2006) (recognizing that “[p]roviding security on the Internet against hacking and other forms of unauthorized use has become a specialized and complex facet of the industry” and ”it is not necessarily the case that safeguards against unauthorized disclosure are inherently stronger when a law firm uses its own staff to maintain a server”).  
116 Google’s terms of service, which are available at http://www.google.com/intl/en/policies/terms/ provides in pertinent part:

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works
At present, twenty (20) states have issued ethics opinions addressing the use of cloud computing or cloud storage. The ABA maintains a list of state ethics opinions.\textsuperscript{117} While there are variations in these ethics opinions, they generally permit the use of cloud computing and cloud storage, but require the lawyer to exercise reasonable care in the selection of a cloud vendor and in assessing the vendor's procedures for safeguarding the confidentiality of client information.\textsuperscript{118} They require a lawyer to evaluate whether a cloud provider's terms of use, policies, practices and procedures are compatible with the lawyer's professional obligations.\textsuperscript{119}

New York opinion 842 explains that exercising "reasonable care" in this context "may" include:

- Verifying the cloud storage provider has an enforceable obligation to preserve confidentiality and will notify the lawyer if served with process requiring the production of client information.

- Investigating the adequacy of the cloud provider's security, policies, recoverability methods, and other procedures.

- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

- Investigating the cloud provider's ability to purge any copies of the data, and to move the data to a different host for any reason.\textsuperscript{120}

Pennsylvania Formal Opinion 2011-200 suggests several other factors that lawyers should consider, including whether the cloud provider:

\begin{quote}
better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services ....
\end{quote}


\textsuperscript{118} See, e.g., N. Y. State Bar Ass'n, Ethics Op. 842 (2010) (concluding that lawyers may ethically use cloud storage so long as they take "reasonable care to ensure that the system is secure and that client confidentiality will be maintained"); Ala. State Bar, Ethics Op. 2010-02 (2010) (determining "a lawyer may use 'cloud computing' or third-party providers to store client data provided that the attorney exercises reasonable care in doing so").


\textsuperscript{120} N.Y. State Bar Ass'n, Ethics Op. 842 (2010).
• Explicitly agrees that it has no ownership or security interest in the data.

• Includes in its terms of service or service level agreement an explanation of how confidential client information will be handled.

• Provides a method for retrieving data if the provider goes out of business, the service has a break in continuity or the agreement is terminated.

• Employs technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing.

• Provides the law firm with the right to audit the provider’s security procedures and to obtain copies of any security audits performed.

• Agrees to host the data only within a specified geographic area.121

On this last point, another state ethics opinion addressing a virtual law practice suggests lawyers should:

[A]ddress and minimize exposure of the client to legal issues triggered by both the international movement, and/or storage, of information in the cloud, and the potential subcontracting out of one vendor’s services to unknown third-party vendors, which may impact confidentiality, without the prior written consent of Attorney and affected clients.122

Pennsylvania Opinion 2011-200 further explains that should the data be hosted outside of the United States, then the law firm should determine that “the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States.”123 It further suggests that a lawyer investigate the cloud provider’s:

• Security measures, policies and recovery methods.

• System for backing up data.

• Security of its data centers and if storage is provided in multiple centers.

• Safeguards against disasters, including multiple server locations.

• History, including the length of time it has been in business, and its funding and stability.

• Process used to comply with data subject to a litigation hold.\(^{124}\)

A lawyer's obligation to confirm that a cloud provider can reliably maintain the confidentiality of client information can be satisfied through "compliance with industry standards," provided those standards "meet the minimum requirements imposed on the [l]awyer" by the State Rules of Professional Conduct.\(^{125}\) A lawyer should verify that the cloud provider will either return or securely delete information from the cloud once an engagement ends or there is no longer a need to retain the information and then evaluate the process to be used to accomplish that task.\(^{126}\) "Otherwise, the lawyer's duty to take reasonable steps to protect the security and confidentiality of that data" will continue indefinitely.\(^{127}\)

A highly relevant inquiry is whether the cloud provider has ever suffered a security breach, and if so, how the breach (or breaches), occurred and what steps have been taken to prevent a reoccurrence.\(^{128}\)

Given the increasing importance of encryption to data security, lawyers should inquire if the cloud provider encrypts information before it is stored in the cloud, if the provider has a process through which client information can be encrypted or if the provider will assist the lawyer to encrypt information before it is stored in the cloud. And if a cloud provider periodically transmits data between servers at remote locations, the lawyer should confirm the data is encrypted while in transit so it remains adequately protected while en route.

---

\(^{124}\) Id.


\(^{128}\) See N. Y. State Bar Ass'n, Ethics Op. 842 (2010) (explaining that if a lawyer learns of a data breach of an "online storage provider," the lawyer must investigate whether the breach involved the client's data, notify any affected clients, "and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated"); see also Alaska Bar Ass'n, Ethics Op. 2014-3 (2014) (noting a "lawyer must notify the impacted client if the lawyer learns that the provider's security was breached and the client's confidence or secret was revealed").
As with any other use of technology, lawyers "should conduct periodic reassessments" of these factors to verify that a cloud vendor's security measures "have not become outdated" in light of changing technology or "that changes in the vendor’s business environment or management have not negatively affected [their] adequacy."\(^{129}\)

Finally, law firms should consider rules and policies that prohibit the use of public clouds by attorneys or staff that have not been carefully evaluated and approved by the firm. This would include the use of mobile technology and applications that store sensitive or confidential client information in public clouds without the firm's prior express authorization.

B. Is Client Consent Required?

Whether client consent is required for the use of cloud computing appears to be an open question. Several of the ethics opinions that discuss the issue suggest that its use may be “impliedly authorized” under Model Rule 1.6 so long as reasonable efforts are used to ensure the data is adequately safeguarded.\(^{130}\)

In an opinion addressing remote access to client files, the New York State Bar Association took the position that when a law firm is able to make a determination that the security measures in place are reasonable, client consent is unnecessary.\(^{131}\) The use of the cloud, however, is just another form of outsourcing.\(^{132}\) Thus, while ABA Formal Opinion 08-451 does not specifically address use of the cloud, it simply cannot be ignored. Opinion 08-451 takes the position that when an outsourcing relationship is attenuated, client consent is required before information covered by Rule 1.6 is shared.


\(^{130}\) See, e.g., Pa. Bar Ass'n, Formal Op. 2011-200 (2011) ("This may mean that a third party vendor, as with 'cloud computing,' could be 'impliedly authorized' to handle client data provided that the information remains confidential, is kept secure, and any disclosure is confined only to necessary personnel."); N. H. Bar Ass'n, Advisory Op. 2012-13/4 (2013) ("As cloud computing comes into wider use, storing and transmitting information in the cloud may be deemed an impliedly authorized disclosure to the provider, so long as the lawyer takes reasonable steps to ensure that the provider of cloud computing services has adequate safeguards."); Nev. State Bar, Formal Op. 33 (2006) (explaining if the third party electronic storage vendor "can be reasonably relied upon to maintain the confidentiality [of client information] and agrees to do so, then the transmission is permitted by the rules even without client consent").


with "outside" entities or individuals "over whom the firm lacks effective supervision and control."\(^{133}\)

One state ethics opinion addressing a virtual law practice that was entirely cloud based explained that the "virtual" attorney:

> [S]hould consider whether her ethical obligations require that she make appropriate disclosures and obtain the client's consent to the fact that an outside vendor is providing the technological base of Attorney's law firm, and that, as a result, the outside vendor will be receiving and exclusively storing the client's confidential information.\(^{134}\)

Several other state ethics opinions suggest that client consent may be required when highly sensitive information is involved.\(^{135}\) New Hampshire, for instance, explains "where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent."\(^{136}\) Ohio State Bar Association's Informal Advisory Opinion 2013-03 appears to echo this view, stating "[i]n exercising judgment about whether to consult with the client about storing client data in 'the cloud,' the lawyer should consider, among other things, the sensitivity of the client's data."\(^{137}\)

The Pennsylvania Bar Association, while not explicitly requiring informed consent, concludes "it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of 'cloud computing' and the advantages as well as the risks endemic to online storage and transmission."\(^{138}\)

---

135 Cal. State Bar, Formal Op. 2010-179 (2010) ("If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent.").
137 Ohio State Bar Ass'n, Informal Advisory Op. 2013-03 (2013); see also Alaska Bar Ass'n, Ethics Op. 2014-3 (2014) ("Where highly sensitive data are involved, it may behoove a lawyer to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent.").
138 Pa. Bar Ass'n, Formal Op. 2011-200 (2011)(further explaining that under Rule 1.4, "adequate information' should be provided to the client so that the client understands the nature of the representation and 'material risks' inherent in an attorney's methods").
Other states' ethics opinions provide more explicit guidance on the issue. Massachusetts Opinion 12-03 addressed the use of Google Docs and concluded that while the use of an internet-based service provider would not violate Rule 1.6 under normal circumstances, a lawyer “remains bound to follow an express instruction from his client that the client's confidential information not be stored or transmitted by means of the Internet, and that he should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so.”139

One of the difficulties surrounding the issue of client consent is that no two cloud applications or vendors are the same. Cloud vendors employ different procedures and safeguards. Moreover, cloud computing has a myriad of potential uses by a law firm. Obtaining client consent for a specific project, such as an e-discovery review platform in litigation or a file sharing application when collaborating on a transaction, is eminently reasonable and can be easily accomplished.

When, however, a cloud based application or computing resource will be used enterprise-wide on an on-going basis by a lawyer or law firm, obtaining client consent may raise a problematic issue. It is unrealistic, for instance, to expect a law firm to have two email systems, one that is cloud-based and a second for those clients that do not consent to the firm's cloud-based email system. So long as a firm has carefully evaluated the cloud-based application, its security and its procedures for safeguarding the confidentiality of client information, the firm should be ethically permitted to use the application.

In light of the quagmire of ethics opinions surrounding the issue of client consent involving a lawyer's use of the cloud, lawyers should carefully evaluate the issue in the context in which the cloud-based application(s) would be used. Given the various ethics opinions noted above, lawyers should carefully address the issue of client consent where highly sensitive information may be involved. Remember when seeking client consent, a lawyer must disclose the risks of using that technology so that the client's consent is "informed."140

Lawyers and law firms should consider addressing the use of the cloud in their engagement letters, explaining how they use the cloud and its potential ramifications in terms that clients can understand. Then a client cannot claim he or she did not know about the lawyer's use of the cloud should a breach occur.

**VII. RECOMMENDATIONS FOR LAW FIRMS ADOPTING A BYOD APPROACH TO MOBILE TECHNOLOGY**

Any law firm that has adopted a BYOD approach to mobile technology should consider developing a comprehensive written data security policy addressing the risks presented by its BYOD program. The policy should address the appropriate use of the mobile devices by the firm's employees, and should clearly spell out that access to the firm's network is conditioned upon full and continuing compliance with the firm's data security policy for mobile devices. The policy should provide that the right to access the firm's network will be immediately terminated if the policy is violated and upon the resignation, retirement or termination of the device's owner from the firm. The policy should further provide that its violation can result in discipline up to and including termination from the firm.

In developing a BYOD program, the firm should also give careful consideration to who will be granted access to the firm's network. Options include all employees, only attorneys, only partners or some combination thereof. To the extent that nonexempt employees of the firm are included, a firm may face wage and hour risk outlined in Part IV above.

The firm should also consider what types of mobile devices will be encompassed by its BYOD policy, which may be influenced by other technology policies the firm has adopted. Should laptop computers or tablets be included or just smart phones? Even though home computers and external storage devices obviously fall outside the parameters of a BYOD policy, the firm should consider including a provision in its mobile device policy that prohibits backing up a mobile device or transferring any firm or client information via a mobile device to a home computer or personal storage device.

Once the type of devices to include in the policy has been determined, the firm should next consider the brands or models of those devices it is willing to support. Relevant considerations include the relative security and continuing viability of various device models and their operating systems, as well as the security of applications that are available from an applicable app store.

Another scope issue to consider is what aspects of the firm's network or what types of data or information an employee will be allowed to access from his or her mobile device. Group policies should be applied to all mobile devices linked to the firm's network with a view to allowing access to only those aspects of the network that are necessary for the particular attorney or employee.

Because lost or stolen devices are one of the major causes of data breaches, the firm's policy should prohibit downloading of any client or firm information on the device. The policy should also require the device owner to immediately report when
any mobile device linked to the firm's network is lost or stolen. Otherwise, the firm will be unable to promptly wipe a lost or stolen device.\textsuperscript{141}

Given the privacy risks outlined in Part IV, the written consent of the device owner to the firm monitoring use of the device, wiping information from the device and obtaining access to it when necessary is a critical feature of any BYOD policy. The policy should also clearly warn the device owner that should remote wiping of the device become necessary, it will likely result in the loss of all personal information on the device.

The policy should also spell out when access to the device itself may be required, \textit{e.g.}, when imposing a litigation hold, in response to a subpoena or governmental investigation, before the device is sold or possession of it is transferred to a third party, or upon the owner's termination or resignation from the firm. The policy should clearly explain the circumstances which will require or permit the firm to wipe the device, \textit{e.g.}, if the device is lost or stolen, if an employee fails to temporarily make the device available to allow client and firm information to be removed before the device is sold or transferred, or upon the owner's resignation or termination from the firm. The policy should further reserve the right to inspect and monitor the device to confirm continued compliance with the firm's mobile device policy. The policy should also advise owners that they have no expectation of privacy in emails or text messages in any device linked to the firm's network or email or information systems.

The firm should consider addressing various inappropriate uses of mobile devices in its policy. Because devices that have been jailbroken or rooted are particularly susceptible to malware, the firm should consider prohibiting attempts to alter or disable any of the device's built-in security features, and to immediately terminate access to its network when it discovers such a policy violation. The firm's policy should prohibit attempts by its lawyers to gain access to the firm's network or systems by using a third party's device. The firm may also want to state in its policy that it prohibits reviewing or sending email or text messages while operating a motor vehicle. A BYOD policy should provide that the firm's other technology policies, such as those dealing with passwords and acceptable use of technology apply to personally owned mobile devices that are linked to the firm's network. Additionally, the firm's BYOD policy should state that the firm's policies prohibiting harassment and discrimination apply to the use of mobile devices, irrespective of where or when an inappropriate use of a device might occur.

\textsuperscript{141} The ability to remotely wipe a lost or stolen device should not be viewed as a panacea by the firm or its lawyers. The ability to remotely wipe the device requires that it be turned on and has battery life remaining on the device.
If the firm prohibits the transfer of firm or client information to the cloud, or permits data to be moved to a firm-approved cloud, that policy should be applied to the use of mobile devices and set forth in its mobile device policy. If a firm has not yet considered cloud issues in its technology policies then it should consider addressing the issue in its BYOD policy since it is likely that at least some of the firm's lawyers have a personal, web-based email account and may have downloaded applications on their device that will automatically store communications and documents in the cloud.

Physically safeguarding the device should also be addressed in the firm's mobile device policy. The policy should provide that the device will remain in the owner's possession and prohibit unsupervised access of the device by family, friends or third parties.

Another critical consideration is the technical safeguards that a law firm will require as a condition of accessing its network. Many devices have MDM applications in the device's operating system and third party MDM applications are available that can be downloaded on the device, which provide the firm with a range of options and even greater controls. MDM applications can allow firms to segregate firm and personal data on the device in separate containers, and depending on the application, allow the device to be configured so as to require one or more of the following controls:

- Strong, complex passwords or biometric security for access to the device;
- Encryption of all data stored on the device;
- Separation and segregation of personal emails, contacts, calendars, notes, reminders and call logs from the firm side of the device to maintain the privacy of the owner's information;
- Locking the device after a specified period of inactivity;
- Wiping a lost or stolen mobile device and/or the use of a remote location feature to find a lost device;
- Locking or remotely wiping the device after a certain number of unsuccessful attempts to log onto the device;
- Prohibiting access to the network by devices that are jailbroken or rooted or unrecognized devices;
- Browser policies that will warn or deny access to certain web sites;
- Data loss prevention policies including data backup restrictions;
- Scanning and assigning risk profiles based to apps on the device;
• Providing a secure tunnel or VPN between the firm side of the device and the
firm's network.

Any technical controls for mobile devices, like those outlined above, that the firm
requires as a condition of gaining access to its network, should be spelled out in its
mobile device policy.

Any BYOD program would not be complete without training. A firm's lawyers
and staff should be trained on its technology policies and its data security policy for
mobile devices. One effective approach to technology training is to personalize the
message. No one wants to be the victim of a cyber-crime or have his or her identity
stolen. Explain that by following the firm's security requirements, they will be
protecting themselves, their families and their loved ones, and in the process will also
be protecting their law firm.

Training should not be limited to the firm's mobile device and other technology
policies but can explain why strong passwords are important, address phishing
schemes, social engineering and other hacker tricks,\(^{142}\) signs that a computer or device
may be infected with malware or may be hacked and who to contact should they
believe that to be true.

Finally a BYOD program is not something that a law firm can roll out with a
policy and then ignore. New applications are being developed on a daily basis and new
vulnerabilities are being identified almost as quickly. Hackers are omnipresent and
developing new attack strategies and modifying malware in an attempt to avoid the
latest technological defenses. A firm's mobile device policy should be periodically
reviewed and evaluated and improved and refined whenever possible. Indeed, the
various ethics opinions discussed above explain that is our ethical obligation.

While a comprehensive BYOD policy, coordinated physical, administrative and
technical safeguards and a robust training program are no guarantee against the risk of
being hacked, they will certainly mitigate that risk. Remember the watch commander's
warning on Hill Street Blues: "Let's be careful out there."

**VIII. SAMPLE LAW FIRM BYOD POLICY**

[INSERT LAW FIRM NAME]

\(^{142}\) The New York City Bar Association recently issued an ethics opinion which expressed the
view that an attorney’s “duty of competence includes a duty to exercise reasonable diligence in
DATA SECURITY POLICY FOR MOBILE DEVICES

The rules governing the legal profession require that lawyers act competently to safeguard information relating to the representation of a client against its inadvertent or unauthorized disclosure and to take reasonable precautions to prevent the unauthorized access of client information. Additionally, HIPAA imposes an obligation to safeguard Protected Health Information (PHI) and various other state and federal statutes require the safeguarding of Personally Identifiable Information (PII). [Some of our clients and insurance carriers are imposing additional security requirements on our Firm.]

Many of the Firm’s lawyers own mobile devices on which email can be sent or received, and information or documents can be accessed, stored or transmitted electronically. While it is not necessary to the performance of legal services, the Firm does allow these personally owned mobile devices to be linked to the Firm’s network, email and information systems as a convenience to our lawyers who may choose to use a mobile device, but are not obligated to do so, when providing legal services to the Firm’s clients. As a result, confidential or proprietary client or Firm information, nonpublic financial information, PHI and PII may reside on these devices or may be transmitted via these devices. The use of these devices can also result in confidential or proprietary information being transferred, uploaded or stored on a home computer, a personal storage device or in a public Cloud outside the protection of the Firm's network, without the approval or authorization of the Firm.

How a personally owned mobile device is used and controlled can impact the privacy and security of the entire Firm and its network and can potentially compromise the Firm's equipment, email and information systems. Malicious applications may be downloaded on a mobile device by its owner, which unintentionally infects the device. Malware can be launched by clicking on links in email attachments or in advertisements on websites which are accessed using the device, which will then attack the device and may seek to access the Firm's network and systems.

Additionally, from time to time it may become necessary for the Firm to preserve and produce electronically stored information (ESI) or emails in the possession of, or under the custody or control of the Firm or its attorneys, irrespective of where that ESI may be stored. As a result, the Firm may need to periodically gain access to a personally owned mobile device, a home computer, a personal storage device, or the Cloud should client or firm information be stored in one of those locations by one the Firm's lawyers. The Firm seeks to avoid, limit, or minimize the need to search home computers, personal storage devices or a non-approved Cloud, and it is in the interests of the Firm and its lawyers to limit or prevent the storage of any Firm or client information on a mobile device, home computer, personal storage device or in any non-approved Cloud.
To comply with various state and federal laws that address the protection of PHI, PII, nonpublic financial information as well as the rules governing the legal profession, which address the protection of client information, attorneys must take reasonable measures to safeguard any information that is either stored, accessed, or transmitted via mobile devices. This data security policy is adopted to protect the Firm's computer network, its information and email systems, and is intended to assist both the Firm and its lawyers in meeting our statutory and ethical obligations to safeguard information. This policy also is intended to prohibit the transfer, upload or storage of Firm or client information to any personally owned mobile device, home computer, personal storage device or non-approved Cloud via a mobile device or otherwise.

Therefore, it is the policy of the Firm that in order for any personally owned mobile device to be linked or granted access to the Firm’s network, email or information systems:

1. The mobile device must be secured by [either (an eight (8) digit PIN,)] (biometrics,) or] a strong password with a minimum of [(eight (8))/(twelve (12))] characters, and must include a combination of capitalized or lower case letters, numbers and symbols at the welcome screen level.

2. The password for your mobile device must [comply with the Firm's password policy,] not be a dictionary word or a word easily guessed by someone who knows you, not include or mimic your name or the Firm's name, be used only for that particular mobile device, and not be used for any other purpose.

3. You agree never to share your password for any mobile device with anyone, to not store any password in plain text on the device or to write down any password and leave it in a place where it can be found.

4. Must be configured so that access to the mobile device is locked out after a maximum of [1/2/3] minutes of inactivity requiring a new login.

5. Must be configured to allow the device to automatically lock [or be remotely wiped] if more than [7/8] unsuccessful logins are attempted to gain access to the device.

6. Must remain in the exclusive possession and control of its owner, and as the owner of the mobile device, you agree not to allow any third person to have unsupervised access to the device, or use it in a way that would permit access to any Firm or client information or any PHI or PII that may be stored on the device.
7. Must be configured so that the device is protected by antivirus/anti-
malware protection that will periodically scan the device or any
applications on the device for the presence of malware.

8. Must be configured so that all information on the device is encrypted.

9. Must have any built-in security features remain in effect on the device.
You agree not to attempt to alter or remove any built-in safety features on
your mobile device and understand that any attempt to alter the device's
built in security, or to jailbreak or root any mobile device that is linked to
the Firm’s network, email or information systems is prohibited.

10. The loss or theft of any mobile device linked to the Firm's network,
email or information systems must be immediately reported to the Firm’s
[Director of IT and General Counsel] immediately upon learning of the
loss or theft of that device.

11. You hereby consent and authorize the Firm to take any necessary
steps to address the loss or theft of any mobile device owned by you that
is linked to the Firm's network, email or information systems, including
the remote wiping (deletion) of any information on a lost or stolen device
by [the Firm’s IT department].

12. The download of any Firm or client information onto a personally
owned mobile device for any purpose is prohibited.

13. The use of any mobile device to send, transfer, store, upload, or backup
any Firm or client information to a home or personal computer, to any type
of personal storage device, or to [(the) (a non-approved)] Cloud is prohibited.

14. The use of any personal, web-based email account on any mobile
device to send, transfer, transmit, store or upload any Firm or client
information is prohibited.

15. You agree to notify the Firm's [Director of IT or (insert person/title)]
before selling, disposing or otherwise transferring ownership, control, or
possession of any mobile device that is linked to the Firm’s network, email
or information systems, and you authorize the Firm to promptly remove
or wipe any Firm or client email or information from the device before [or
after] selling, disposing or transferring ownership, control, or possession
of the device.

[16. Because using the voice-to-text feature of a mobile device can result in
the transmission of the spoken words to a third party for review and
analysis, you agree not to use the voice-to-text feature of your device to]
draft or send any email or text messages related to a Firm matter, or a Firm client, or that relates or includes the content of any PHI, PII or nonpublic financial information.]

[17. Reviewing or sending email or text messages while operating a motor vehicle is prohibited.]

*It is the policy of the Firm that access to the Firm’s network, email and information systems will be blocked immediately upon the effective date of a person’s resignation or termination from the Firm.*

The obligation to preserve client information survives an attorney’s departure from the Firm, and an attorney must continue to safeguard the information stored on any mobile device after the attorney is no longer employed by or associated with the Firm. You agree that the Firm’s IT department can remove any client, Firm, or work-related, email, or information on a mobile device upon notification of a person’s resignation or departure from the Firm. Any attorney or person who resigns from the Firm or is involuntarily terminated by the Firm must temporarily turn the device into [the Firm’s IT department] and allow the removal of any Firm and client information or emails from the device. If a person who is terminated or resigns from the Firm refuses to temporarily turn his or her mobile device into [the Firm’s IT department] for the removal of Firm or client information and emails from the device, the Firm reserves the right to remotely wipe that information from the device, and you hereby consent to having the device wiped, and understand that wiping the device could potentially result in the loss of any personal information you stored on the device.

The failure to follow the Firm’s policies on mobile device security can result in discipline up to and including separation from the Firm. A violation of this policy can also result in the immediate termination of your access to the Firm's network, email or information systems via your mobile device.

All other Firm policies including the acceptable use of technology and those prohibiting harassment and discrimination apply to your use of a mobile device and all partners and employees must adhere to them when using a mobile device covered by this policy.

**Consent:** I understand that as a condition of the Firm allowing me to use a personally owned mobile device to gain access to the Firm’s network, email and information systems, I agree to follow the Firm’s data security policy for mobile devices, and I expressly consent and hereby authorize the Firm to take whatever steps may be necessary to address the loss or theft of any mobile device that I own, which is/are linked to the Firm's network, email and information systems, including the remote wiping (deletion) of information contained on my device(s) by [our Firm’s IT department]. I further consent and hereby authorize the Firm to remotely wipe the device in the event I resign or am terminated from the Firm and refuse to temporarily
turn the device into [the Firm’s IT department] to allow the removal of Firm and client information and emails from the device. I further consent to allowing the Firm to remove or wipe any Firm related emails or information and any client related information from the device before I sell or transfer possession of the device or should I refuse to temporarily turn the device into [the Firm’s IT department] to allow the removal of Firm and client information and emails from the device. I understand that wiping the device could result in the loss of any personal information stored on my device.

I acknowledge and understand that if I do not secure and configure, or allow the Firm to secure and configure any mobile device as outlined in this policy, and if I do not consent to the remote wiping of any such device(s), that my access to the Firm's network, email and information systems through any such device(s) will be blocked or terminated.

I further consent and hereby authorize the Firm to recover any Firm or client-related emails or documents from any Cloud, home computer or personal storage device to which those emails or documents were uploaded or stored in violation of this policy. I also consent to the periodic inspection of any mobile device connected to the Firm's network, email or information systems to ensure compliance with this policy.

Dated: ______________

(Print name)

(Signature)

* Steven M. Puiszis is a Partner with Hinshaw & Culbertson LLP, and serves as the Firm’s Deputy General Counsel. He is a member of Hinshaw’s Lawyers for the Profession Practice Group which represents lawyers and law firms in liability and professional responsibility matters. Steve also serves as the Firm's privacy and security officer. He is a Fellow of the American Bar Foundation and is a Past President of the Illinois Association of Defense Trial Counsel. He formerly served on the Board of Directors of DRI and as its Secretary Treasurer. His publications include DATA PROTECTION AND PRIVACY IN THE UNITED STATES, and MITIGATING LAW FIRM’S CYBER RISK; separate book chapters published in RISK MANAGEMENT IN LAW FIRMS, Globe Law and Business Publishing Ltd., London, England, sponsored by the International Bar Association; THE ROLE OF GENERAL COUNSEL IN LAW FIRM RISK MANAGEMENT, LAW FIRM PRACTICE MANAGEMENT, the DRI Defense Library Series, DRI, Chicago, Illinois. Steve received his J.D. from Loyola University Chicago.