ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Bring Your Own Device Workforce is Upon Us All: Leverage it!

Compliance and Ethics

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Marry the technical with the legal.*** A comprehensive BYOD policy must be legally sound within the laws of your jurisdiction, but provide minimal disruption to the business.
- ***Obtain buy-in.*** Find time to secure feedback from senior leadership to reduce the risk of conflict, as well as regular employees to ensure that they understand what they're signing up for.
- ***Know your local laws.*** Potential areas of risk include overeager monitoring of employee data, issues of compensation related to hourly workers, and discrimination suits.
- ***The times they are a-changin'.*** It's likely that the legal backdrop will change between the time a business agrees to a BYOD policy and when it completes a draft.

The number of mobile device users continues to be on the move — and it's exponentially up. According to the Pew Research Center, nearly two-thirds of Americans own a smartphone. That's up from approximately 35 percent in 2011, representing substantial and sustained growth in this market. This fact alone certainly helps to substantiate that this recent, explosive growth has a strong foundation and is quickly becoming an engrained aspect of everyday life for many. However, the global statistics are even more astonishing. By 2016, it is predicted that over 480 million smartphones will be shipped worldwide. Of that number, 65 percent — or 312 million smartphones — will be used for BYOD purposes. Similarly, it is also predicted that over 370 million tablets will be produced worldwide in 2016. As such, it is no wonder that 46 percent of smartphone owners say their smartphone is something "they couldn't live without."

Thus, to poorly assume that all — or even most — of these smartphone users are living without their smartphone during work hours or while at work is nonsensical. Moreover, whether sanctioned or not, some of these smartphone users and other mobile device users are conducting the business of their organization on their mobile devices. That is why, by 2017, it is expected that two of out every three companies across the world will adopt a specific Bring Your Own Device (BYOD) policy and solution.

As a whole, these statistics and trends indicate forthcoming innovation and transformation in the workplace. In addition, the change carries risk for employers, which must be mitigated to reap the rewards which the technology continually yields. As a result, each and every employer should address the issue of the BYOD workforce in some form, or they will chance being left in a position of potential liability without having taken the opportunity to address and/or remediate BYOD workplace issues. Therefore, this article attempts to provide in-house counsel with a high-level approach to creating and designing a BYOD policy, while balancing that approach with an update from a sampling of current international law.

Designing a BYOD policy

In a BYOD workforce, employees use their own mobile devices whether they are laptops, tablets, smartphones, etc., in their everyday life as well as for work purposes. At first thought, a BYOD workforce sounds great. Employees can use their devices to be both productive for work and continually accessible in their personal life. Employers get the added benefits of effects like leveraging more technology, possibly increasing employee retention and cutting bottom line costs. However, the risks with such a workforce have significant impact to both employees and employers from a multitude of legal perspectives. Therefore, a strategy to creating a BYOD policy that incorporates diligence and a structured approach is most likely to have success. As such, this article provides the following high-level approach to getting started.

Prepare and decide

The purpose of a BYOD policy is to establish authorized organizational processes and procedures for employees who wish to use employee-owned mobile devices for work purposes. A successful policy minimizes employer and employee risk and exposure, and it clearly delineates the legal considerations of such an organizational initiative by informing both parties how the policy impacts the control and usage of the employee's mobile device.

Therefore, before moving further, an organization must first decide whether it should implement a BYOD policy. To ensure that all aspects of day-to-day operations are considered, the organization must ensure that all the key decision-makers for the organization have a seat at the table. In most instances, if available, this should at least include the information security officer, human resources officer, in-house counsel, and compliance officer. Each of the aforementioned plays an integral role in providing valuable input and assessing the risks surrounding a BYOD policy. Irrelevant of specific roles, the organizational team must be able to properly assess, address, and communicate security requirements for mobile devices, authentication requirements, employer liability, usage restrictions, a support model, encryption requirements, and acceptable uses. If your organization does not have the internal resources to take on this work, then it may look to the plethora of available external consultants and/or counsel as a starting point.

After proper time and consideration is given to preparation, the organization must make the decision and commitment to create a flexible and enforceable BYOD policy. That decision must be classified and regarded as an organizational initiative, not a solemn departmental project. To that end, the organization must begin by allocating and accounting for an ample amount of time and financial and human resources, including properly skilled internal or external personnel, to achieve success.

Survey the aspects of a BYOD policy

After the decision is made to create a BYOD policy, an organization should survey the aspects, both technical and legal, of a BYOD workplace. This survey should be as comprehensive as possible. As a starting point, the survey could evaluate the following questions:

- **Business goals:** What is the specific purpose for the organization to have a BYOD policy? Is it solely for improving employee quality of life? Is it solely to increase employee productivity? Is it a balance between the two? And what are the measurable results that the organization can track, analyze, and assess during implementation and rollout to measure whether the purpose is being achieved?
- **Existing policies:** What are the existing policies that will, or incidentally could, impact a BYOD workforce? What are the advantages and disadvantages of those policies? At the crossroads of the existing policies and the to-be BYOD policy, where is it best to address converging issues? Which policy should be updated?
- **Acceptable risks:** Who will comprise the organization's BYOD workforce (exempt vs. non-exempt employees)? Where do these employees work? Where do these employees reside? How and where is the organization legally organized? In what sector does the organization conduct business? Is that sector regulated? Where will employees use their device? Will organizational data cross international borders? If so, which ones?
- **Impacts to the business:** What types of business functions will be permitted on a BYOD device? Will business functions be limited to email? Will business functions also allow file sharing? Will employees be permitted to use BYOD devices after work hours for business

purposes? If so, how will the organization manage hours worked and wage considerations? Will employees be reimbursed or provided a stipend for providing an employee-owned device for use? Are there third-party contracts that could impact the policy?
- **Technology considerations:** Which devices will be permitted to be a part of the BYOD workforce? What are their respective minimum operating system requirements? What device security will be required? How will device security be implemented and monitored? Will security updates be pushed to the devices? Will organizational and employee data be partitioned on the mobile device? How will backup of organizational and employee data occur? What is the disaster recovery plan and how it will be executed?

During the survey process, legal counsel should be involved as much as possible for their legal advice on the issues and decisions at hand. This helps to ensure that attorney-client privilege is addressed and that the communications, which are properly subject to the privilege, may be protected from discovery. Furthermore, legal counsel can provide beneficial business acumen to communications. By using their knowledge of the organization's structure, culture, and other organizational aspects, they can assess and assist in managing the risks that the organization may confront. However, as always, in-house counsel should always be mindful when providing business advice as it may erode future claims to privilege.

Draft a BYOD policy

After the survey process is complete, the drafting can begin. In general, the draft should outline the duties, obligations, and roles and responsibilities of both parties — employer and employee. It should explain, in plain language, the security of data and the information systems that are impacted. For a list of key provisions, please see the sidebar below.

HERE ARE A FEW KEY PROVISIONS TO CONSIDER DEPENDING ON THE PURPOSE OF THE BYOD POLICY:

- Policy scope
- Policy acknowledgment and enforcement
- Required user security awareness training
- Acceptable uses (both personal and work), which assists both parties in limiting their exposure to data breaches, mitigating risk related to potential liability, and increasing organizational productivity
- Security — physical, password, and third party use
- Policies regarding passwords, wireless access, remote access, remote working, and incident response measures
- Device and operating system versions requirements, which should include their respective updating and security monitoring
- Seizure of an employee's data or device
- Information classification — organizational and personal
- Impact to other organizational policies, such as Human Resources' specific policies
- Virtual Private Network (VPN) access and configuration
- Employee compensation

While it will not eliminate the myriad of legal issues that may present themselves from a BYOD workforce, taking the time to draft a properly written BYOD policy will ensure that the policy is effective to address the relationship between employer and employee, and it will likewise assist in responding to any issues that may arise. Furthermore, seeking feedback from senior organizational leadership will help reduce the chance of a conflict within your organization. In seeking such feedback, ask the reviewers to read the draft from the perspective of both employee and employer, as they will more than likely serve in both capacities regarding the BYOD policy.

Review and address the current legal landscape before publishing

Without question, the legal landscape will change from the day an organization decides to establish a BYOD policy to the point when it prepares a viable draft. Therefore, reviewing and addressing any recent changes in applicable law is another important aspect of the BYOD policy creation process. Some of the areas of law impacting employee-owned mobile devices include intellectual property law, patent law, and criminal law. This article, however, seeks to survey current law, from across the world.

In the United States, two federal laws that present large BYOD workplace risks to employers are the Computer Fraud and Abuse Act, as amended, (CFAA) and the Stored Communications Act (SCA), Title II of the Electronic Communications Privacy Act of 1986 (ECPA).

The CFAA was enacted in 1986 as part of a movement to better address computer fraud law. For employers, it has two substantial impacts. First, it imposes penalties on individuals and organizations that “intentionally access a computer without authorization or exceed authorization, and thereby obtains … information from any protected computer.” Second, the CFAA also prohibits individuals and organizations from “knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer.” Penalties imposed on organizations for CFAA violations can include a fine of not more than US$200,000 for the first offense, and fines of not more than US$500,000 for subsequent violations.

By a similar token, the SCA prohibits intentional unauthorized access to employee’s personal electronic communications. Specifically, it provides that “whoever intentionally accesses without authorization a facility through which an electronic communication service is provided … and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage … shall be punished as provided.” Like the CFAA, the SCA includes a civil action and criminal punishment. Thankfully, it permits access to a stored communication when consent is provided by the user.

By taking a few steps, organizations may mitigate their exposure to the CFAA and the SCA. First, organizations must secure employee’s affirmative consent to the BYOD policy. Two methods for doing so are having the employee (1) sign a form or (2) accept the policy electronically by clicking on an acceptance box. Second, records of acceptance should be retained permanently. Third, they should also be producible upon request. Finally, organizations should assess their positions on personal content (i.e., when can they view personal content; should they back up personal content as part of a disaster recovery plan; when are they able to wipe content — personal and business related — from a mobile device; etc.) and then clearly, in plain language, communicate their position to employees via the BYOD policy.

Contrast the aforementioned with applicable federal laws from Germany, which has some of the most

stringent data security and privacy laws regarding employee-owned devices in the world. To illustrate the importance its culture places on the topic, in addition to its federal laws, every state within its borders has its own data protection law on point. However, one particularly applicable German federal law is Germany's Federal Data Protection Act (BDSG), more appropriately known as Bundesdatenschutzgesetz, which implements Directive 95/46/EC on data protection. The BDSG seeks to protect personal data (including employee data) from processing and use by private and public authorities located and not located in the European Economic Area (EEA), which collect, process, or use personal data in Germany. Among other specific regulations, the BDSG requires users must abide by the data protections principles of data reduction and data economy, explicit permission, purpose, direct collection, access, accuracy, and limitation. The BDSG and its principles are strictly enforced in this jurisdiction, and violations thereof include, but are not limited to, fines, criminal offenses punishable by imprisonment, civil liability, and injunctive relief.

Given Germany's recent, stringent stance regarding data protection, it is reasonable for employers to, expect that other similar federal laws will be abounding internationally. However, keeping up with new international federal law is not the only daunting thing in this legal space. For example, in the United States, there is a plethora of state court decisions emerging on the topic. In contrast, there are also countries like France, which have neither federal nor case law on point. Therefore, this article also explores a few BYOD employment law issues and seeks to evaluate how employers act after evaluating applicable state case law from the United States and the most applicable French law.

Under the United States' Fair Labor Standards Act (FLSA), employers must compensate non-exempt employees for out-of-office time worked that benefits the employer, including overtime pay. As one can foresee, a BYOD workforce can work from anywhere at any time. For the employer, this means that minor tasks that were previously considered *de minimis* can be in fact compensable.

As an example, the court in *Allen v. City of Chicago* recognized the existence of such compensation in a class action lawsuit. There, the court certified a class of employees who were "required to use" employer-issued devices to perform work outside of normal working hours. These employees did not receive compensation for their time even though the work was "routinely and regularly accomplished" through the use of the devices. In a more recent decision, the court in *Mohammadi v. Nwabuisi* held an employer liable for uncompensated work hours. In that case, the employee not only performed overtime work from his personal device, but he also did so from his personal email address.

In France, one would expect the result to be the same. There, similarly situated French employees as those described in the aforementioned cases would almost certainly need to be compensated. While there is not a specific law on point, this conclusion is drawn from deduction. Under French law, employees must disconnect from remote working devices during rest periods, and employers must ensure the means are available for employees to do so. Furthermore, under French law, the working day may not generally exceed 10 hours. If it does, the employer owes the employee specific overtime payments. Therefore, it is reasonable to deduce that a French employee completing *de minimis* tasks from an employee-owned device after hours would need to be compensated.

Therefore, to address these potential wage claim issues like the above, organizations should strongly evaluate which employees are authorized to participate in their BYOD workforce. In the United States, one approach could be to limit BYOD participation to exempt employees. As such, when drafting a BYOD policy, organizations should know and further evaluate the distinction between exempt and nonexempt employees, which has been a source of litigation. Across the globe, a good starting point would be to limit the practice to employees who are critical to the organization's

mission and goals. In both instances, it is quickly becoming a best practice to create time reporting systems such that all time worked, including the time that occurs after normal working hours, is able to be recorded and paid accordingly. Another BYOD employment law issue that has been addressed and is sure to be addressed even more in the future is that of employee reimbursement for BYOD workforce participation. As expected, many employers address the issue of reimbursement, whether it is a full or partial reimbursement. However, as likewise expected, there are employers who do not reimburse employees at all. In the State of California, this is a problem.

In *Cochran v. Schwan's Home Service, Inc.*, the court held that California labor law requires employers to reimburse employees who are required to use their personal cellphones for work-related purposes. Specifically, the court stated:

"We hold that when employees must use their personal cellphones for work-related calls, Labor Code section 2802 requires the employer to reimburse them. Whether the employees have cellphone plans with unlimited minutes or limited minutes, the reimbursement owed is a reasonable percentage of their cellphone bills."

While California state law is certainly not binding on organizations outside its jurisdiction, such a ruling provides point of view on how prospective courts could view similar cases. Therefore, organizations should consider whether they are reasonably reimbursing their employees for BYOD participation. This evaluation should also include employees who previously had unlimited minutes prior to becoming a participant in the organization's BYOD workforce. Therefore, employers should evaluate whether their respective jurisdiction takes a similar approach to California's.

Finally, some courts and laws have addressed the BYOD employment law issue of employer liability related to discrimination claims. In *Espinoza v. County of Orange*, the court held an employer liable and awarded over US$820,000 in damages for harassment in the form of cyberbullying. In that case, employees continually posted comments about a coworker's disfigured hand to a non-employer blog. While the employer had knowledge of the blog and the ongoing actions by its employees, the employer failed to remediate. In addition, its knowledge came from the fact that employees were accessing the blog from its network.

Similarly, the court in *Blakey v. Continental Airlines, Inc. et al.* found the defendant and employer liable for harassment involving an online, workplace message board. There, the employer operated a website to provide employees the option to login and review relevant workplace information. In addition, there was a message board for employees to communicate on. However, some employees used the message board to harass the plaintiff, an employee. In finding the employer liable, the court stated that "employers do not have a duty to monitor private communications of their employees; employers do have a duty to take effective measures 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."

As a result of both decisions and others like it, employers operating in the United States are now being held liable for discrimination claims where they are inappropriately monitoring employee activity on employee-owned devices. Therefore, employers should take measures to address and reasonably monitor such activity. The monitoring should not focus solely on access and activity performed from the organization's network. Rather, it should reasonably evaluate, in light of applicable privacy law, employee access and activity on employee-owned devices used for work purposes.

Discrimination in the employment law context is also prohibited in France. While there is neither

French federal nor case law on point specifically regarding BYOD discrimination issues, French employment law prohibits workplace discrimination generally. Further, it specifically prohibits discrimination against employees during the employment relationship and even in the recruitment process. Applied to the employee-owned device context, this yields an interesting result. It requires hat employers not evaluate and use neither an applicant's ownership of a device nor the applicant's desire and willingness to use his or her device at work as a hiring condition. In addition, it further requires that the same apply even during the employment relationship. Therefore, as BYOD laws and decisions like the aforementioned continue to evolve globally, employers must ensure that employees are not discriminated, harassed, or retaliated against by other employees on employee-owned devices, nor should employers use an applicant's or an employee's employee-owned devices as a basis for discrimination.

Conclusion

In sum, the BYOD workforce is very real. For employers and employees, the legal issues related to a BYOD workforce continue to evolve. As such, more litigation, regulation, and court rulings are forthcoming and will soon receive our attention. Thus, it can be expected that the future costs related to the aforementioned will increase. However, with a well-drafted, flexible, and enforceable BYOD policy that is frequently reviewed in light of the ever-changing legal landscape, organizations can maximize their rewards, mitigate their risks, reduce their exposure to litigation, and hopefully retain highly-productive employees.

Further Reading

18 U.S.C. §1030.

18 U.S.C. §2701.

18 U.S.C. §1030(2)(C).

18 U.S.C. §1030(5)(C).

18 U.S.C. §1030(c), 3571.

18 U.S.C. §2701(a)(1).

18 U.S.C. §2701(b).

18 U.S.C. §2701(c)(2).

Allen v. City of Chicago, 20 Wage & Hour Cas. 2d (BNA) 1124 (N.D. Ill. 2013).

Mohammadi v. Nwabuisi, 990 F. Supp. 2d 723 (W.D. Tex. 2014).

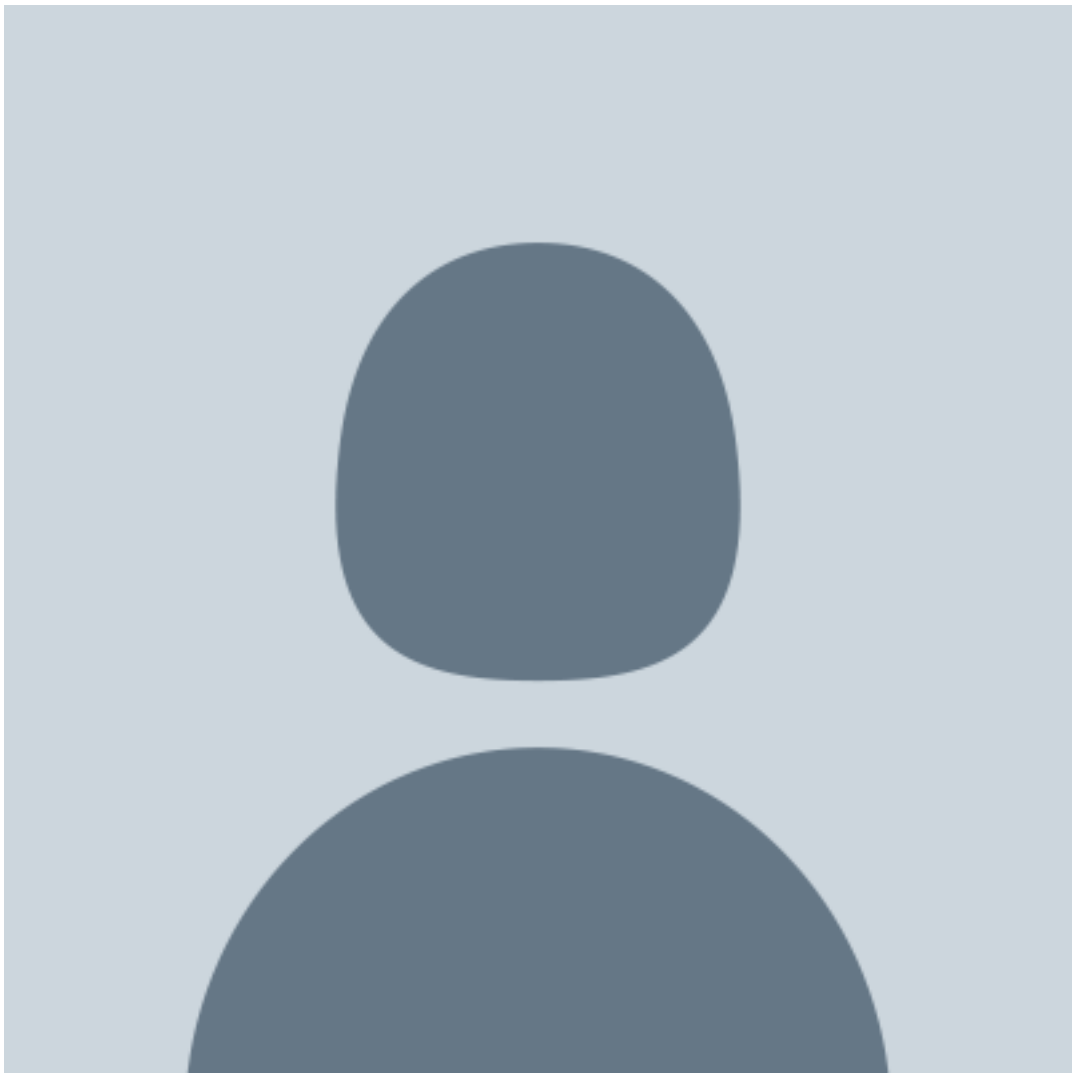
Cochran v. Schwan's Home Services, Inc., 228 Cal.App.4th 1137 (2014).

Espnioza v. County of Orange, 2012 WL 420149 (Cal. App. Ct. Feb. 9, 2012).

Blakely v. Continental Airlines, Inc. et al., 751 A.2d 538 (N.J. 2000).

SYNTEC National Collective Bargaining Agreement (CBA) of France.

Josh E. Torres



In-House Counsel

Hibbett Sporting Goods, Inc.

He is also treasurer and secretary of the ACC Alabama Chapter.