eDISCOVERY BEST PRACTICES:
BYOD POLICIES AND EMPLOYEE RIGHTS

The use of personal devices to conduct nonpersonal business has become increasingly common. In addition, corporations are issuing mobile devices that employees may use for personal activities. Therefore, organizations should understand their needs, rights, and obligations, and the rights and expectations of employees, when evaluating and implementing "bring your own device" policies and programs or issuing devices that can be used for both business and personal matters.

"An effective BYOD policy enables mobile workforce productivity while securing company confidential and proprietary information," said Randy Diamond, director of library and technology resources and legal research professor at the University of Missouri School of Law.

"The policy should support the client's business objectives and comply with the regulatory environment in which the company operates. Trouble arises when policies do not establish clear rules and boundaries governing employee use of their own or company-enabled devices for business use."

"An effective BYOD policy enables mobile workforce productivity while securing company confidential and proprietary information."

UNDERSTANDING PRIVACY RIGHTS

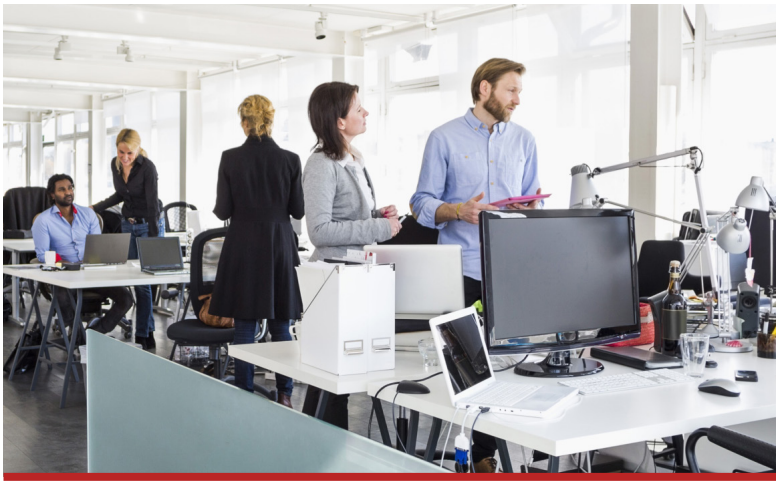
A company's ability to access data on an employee's device will be affected not only by the technologies adopted but also by employee and third-party privacy rights in data and files stored on the device. Federal and state laws, such as the Health Insurance Portability and Accountability Act, as well as common law privacy principles, require the protection of health, financial, and other personal, confidential information. In addition, international privacy and discovery and litigation laws may come into play, depending on the country in which a company is operating or the location of the device.[1]

"*Crabtree v. Angie's List* [2] is a civil litigation example of cellphone privacy concerns the U.S. Supreme Court articulated in *Riley v. California*,[3]" Diamond said. "In *Crabtree*, the court denied defendant's request for a forensic examination of employee personal cellphones to obtain GPS and location services data, finding the request was disproportionate to the needs of the case and outweighed by the employees' significant privacy and confidentiality interests."

Local, state, federal, and international law govern the ability to access ESI from employee mobile devices.

In addition to U.S. and international common and statutory law, employers in the public sector may also be limited in their access to mobile devices because of the application of federal and state constitutional provisions.[4] Further, statutory and constitutional protections may apply not only to the employee in possession of the mobile device but also to third parties whose information may be stored on it. Employers should keep these limitations on access in mind when crafting BYOD programs and policies.

BALANCING CORPORATE NEEDS WITH PRIVACY



When considering the implementation of BYOD programs and policies, employers should first understand relevant security issues for their company and business sector.[5] Risks to consider include data leaks or breaches leading to the release of sensitive company information or third-party personal information and the introduction of malware or spyware to the mobile device or the company network.[6] They should also be familiar with the implications of being unable to access business information on employee-owned devices with respect to litigation (discovery) and regulatory compliance,[7] and should prepare program requirements and policies taking these concerns into account. Requirements and policies should be clearly communicated, and employees trained on program requirements.

Employers should also consider the types of litigation and discovery challenges that may arise in the context of BYOD programs. Most courts weighing in on the issue have found that data on BYOD is subject to the same preservation obligations as other electronically stored information.[8]

"Major discovery challenges can [arise] from lapses in sound BYOD practices," Diamond said.

"Litigation holds must account for employee mobile devices. *In re Pradaxa*[9] is a classic illustration of the loss of relevant text messages resulting from the company's failure to properly implement its litigation hold to prevent automatic deletion of employee text messages. Clear communication with employees about company discovery obligations, including timely preservation of ESI on mobile devices, is critical when a duty to preserve arises."

Several factors influence whether information on an employee-owned device is discoverable and subject to a litigation hold. These factors include, but are not limited to, whether the information is within the employer's possession, custody, or control; whether company information is segregated from private information and the way information is stored; whether the information is unique; and whether the discovery of the information is proportional to the needs of the case.[10]

Most courts have found that BYOD data is subject to the same preservation obligations as other ESI.

Finally, employers should address situations in which the company is not a party to the litigation but must protect company information on the employee's device from discovery in litigation not involving the employer.[11]

USING DEVICE MANAGEMENT SOLUTIONS

Employers should use available technology to proactively manage employee-owned devices. Mobile device management, also known as MDM, and enterprise mobility management, or EMM, are two ways to manage and secure employee mobile devices. While the terms are still used somewhat interchangeably, MDM generally refers to the ability of companies to manage an employee's device at a global level. For example, if an employee reported losing a cellphone containing sensitive corporate information, an MDM solution would often consist of wiping the device of all data, while an EMM solution would remove only company-specific information.

Specific solutions include separating business information from personal information. "By 'containerizing' business and personal data, the company will reduce or head off common discovery headaches involving company possession, custody, and control issues of current and former employee business data," Diamond said.

POLICY PROVISIONS TO CONSIDER

When considering or implementing a BYOD program or policy, initial consideration should be given to the types of data, and associated risks, that will be made accessible to mobile devices. Other aspects of a successful BYOD program include, among other things:

- Documenting the process for granting BYOD access
- Detailing acceptable use provisions
- Detailing requirements for software updates
- Requiring reporting device loss or theft

- Proactively informing employees of the possibility of data wiping (and requiring acknowledgment in writing)
- Requiring passcodes for access to company data (4-digit pins are insufficient)
- Detailing encryption and other security issues, such as whether it is permissible to use public Wi-Fi
- Putting in place controls to properly backup firm data

In addition to crafting careful policies and employing appropriate technologies for active employees, employers must plan for situations in which employees leave a position, whether voluntarily or involuntarily. If a company has not implemented processes for containerizing company data away from employee data, this may include wiping the leaving employee's entire device.[12]

"By 'containerizing' business and personal data, the company will reduce or head off common discovery headaches."

"Careful observance of employee exit procedures and protocols should include termination of BYOD privileges and the company's right to extract or recover business data and business devices when employment terminates," Diamond said. "Employee education and ongoing training and policy reminders are essential for successful policy implementation and observance."

POLICIES SHOULD EVOLVE WITH TECHNOLOGY

While employers should consider all the above when crafting BYOD programs and policies, they should also remember that technology changes almost daily.

Asked about future developments in the area of BYOD and other "bring your own" areas, Pete Haskel,[13] of counsel at Bojorquez Law Firm and a member of The Sedona Conference Working Group on Electronic Document Retention & Production, said, "I sense a growing consensus that any current BYOD policy likely soon will be overtaken by two accelerating trends: the weakening of distinctions between personal and business communications, and technology advances that multiply the types of available communications and storage devices. "

"For example," he said, "how will any BYOD policy address employees using embedded chips that they wear instead of carrying a smartphone? Barring some startling technology advances in security measures, I think employee training and discipline will become ever more effective compared to technology measures as the most important component of BYOD policies."

Careful thought regarding legal requirements, in addition to collaboration between legal and IT departments, is necessary for any successful BYOD policy. Thoughtful planning will ensure that employees understand the do's and don'ts of company BYOD policies, will ensure that the company has processes and people in place for monitoring technological and personnel changes, and will ensure that best efforts have been made to protect sensitive and confidential information through security protocols. Lastly, companies should understand that creating and implementing a BYOD policy or program is not a static process but rather is an ongoing endeavor that changes as technologies change.

ABOUT CANON DISCOVERY SERVICES

Canon Discovery Services has a skilled, dedicated team of discovery professionals with a proven track record in solving complex discovery matters. Backed by over twenty years of experience, we help law firms and corporate legal departments develop practical, defensible eDiscovery response plans to support successful outcomes. Our services range from ESI processing, culling and analysis, document review, hosting and production to implementing information governance and readiness response programs. Canon Discovery Services is a part of Canon Business Process Services, a subsidiary of Canon U.S.A. Visit us at cbps.canon.com.

---

[1] The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495, 526 (forthcoming 2018), available at https://thesedonaconference.org/publication/Commentary%20on%20BYOD

[2] No. 1:16-cv-00877-SEB-MJD, 2017 WL 413242 (S.D. Ind. Jan 31, 2017)

[3] 134 S. Ct. 2473 (U. S. 2014) (unanimous decision regarding Fourth Amd. search and seizure considerations in cellphone context)

[4] *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010) (city employee had a reasonable expectation of privacy under the Fourth Amendment in text messages even though the cellphone was issued by the municipality)

[5] Andrew Hinkes, "BYOD Policies: A Litigation Perspective," American Bar Association, Section of Litigation, July 8, 2013, https://www.americanbar.org/groups/litigation/committees/corporate-counsel/articles/2013/spring2013-byod-policies-a-litigation-perspective.html

[6] Allyson Haynes Stuart, "Making Sure BYOD Does Not Stand for 'Breach Your Organization's Data,'" 27 S.C. Law. 45, ** (March 2016) http://mydigitalpublication.com/publication/?i=292814&article_id=2415879&view=articleBrowser&ver=html5#{"issue_id":292814,"view":"articleBrowser","article_id":"2415879"}

[7] The Sedona Conference, "Commentary on BYOD," see generally pp. 512-515 and 528-532 (discussing implications related to inability to access devices and considerations for obtaining access)

[8] Beth S. Rose, "E-Discovery and Bring Your Own Device to Work: The New Norm," Sills, Cummins & Gross, October 2015, p. 1 (collecting cases)

[9] *In re Pradaxa Products Liability Litigation*, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013), rev'd on other grounds, *In re Petition of Boehringer Ingelheim Pharmaceuticals, Inc.*, 745 F.3d 216 (7th Cir. 2014)

[10] The Sedona Conference, "Commentary on BYOD," pp. 528-37

[11] Ibid., pp. 546-47

[12] Kenny Leckie and Nik Prosser, "The Practices, Pitfalls, and Policies of a Post-BYOD World," *Peer to Peer*, The Quarterly Magazine of ILTA, Fall 2015, pp. 13-14, http://epubs.iltanet.org/i/588021-fall-2015/4

[13] Mr. Haskel's comments reflect his views and not the views of his firm or the organizations of which he is a member.