Bring Your Own Device (BYOD) . . . at Your Own Risk [1]

1. What is BYOD?

2. What are an employer's concerns surrounding BYOD?
   A. Legal obligations
   B. Security
   C. Protecting data for other business purposes

3. What might employees expect to find in BYOD policies?
   A. Permitted and prohibited uses, devices, and software
   B. Employee responsibilities
   C. Explanation of available/required technical support
   D. Consent to certain practices
   E. Explanation of mobile device management software

4. Why are employees concerned about their privacy?

5. Tips for employees considering participating in a BYOD program.
   A. How employees can protect their privacy proactively
   B. When employees believe an employer has violated their privacy

6. Tips for employers implementing a BYOD program.

7. Additional resources.

1. What is BYOD?

In the not too distant past, employees had no choice but to work at a company's office or on a company laptop or phone. As mobile electronic devices (tablets and smartphones, for example) became both more accessible and affordable, this changed. Now employees can work virtually anywhere and it's becoming more and more common [2] for them to use devices for both personal and work purposes.

Many individuals own multiple mobile devices. One person may own a smartphone, tablet, and laptop computer. An employer may also offer employees one or more company-owned devices. For some, it's both inconvenient and less productive to carry company-issued and personal devices. Others may prefer a specific technology or brand, or simply be annoyed by having to carry multiple devices.

If an employer doesn't offer employees the option to use a company smartphone, tablet, or laptop, employees may still want the option to work remotely. This work could include accessing work files, the company network, the phone system, emails, and even contacts.
Bring your own device (“BYOD”) policies are making a significant impact on the workplace. Employers create BYOD policies to meet employee demands and keep employees connected. They may also do it to save money by eliminating the need for company plans and devices.

While "bringing your own device" is common, allowing employees to use personal devices for business purposes can expose employers to many risks. Because of these concerns, employers often establish BYOD terms or policies that can have a surprising and significant impact on employee privacy. However, not all employers have BYOD policies even though employees may already be using personal devices for work purposes.

This Fact Sheet addresses reasons employers have BYOD policies, some practices employees may encounter, and some of the common concerns and privacy risks that employees face when considering whether to participate in an employer's BYOD policy.

2. What are an employer's concerns surrounding BYOD?

Employers will assume legal, security, reputational, and other business-related risks when their employees use a device for both personal and work-related purposes. This is largely because employers lose control when employees use their own devices and networks to store and transmit company data. The same is true when employees use company-owned devices for personal purposes.

A company may need to protect many types of sensitive information for business and/or legal purposes. Sensitive information might include:

- human resources information,
- health information,
- confidential or privileged information relating to legal matters,
- financial information,
- proprietary information and trade secrets, and
- client or marketing lists.

A. Legal obligations

There are many laws and regulations companies must consider when creating a BYOD policy. Which laws apply will depend on the nature of the employer's business and what kind of data it collects, stores, and uses. Some industries, such as healthcare and finance, are subject to more legal obligations than others. An employer's legal obligations may include, but are NOT limited to:

- **State and federal security breach notification laws.**
  These include federal industry-specific laws rules such as the Breach Notification Rule under the Health Information Portability and Accountability Act (HIPAA). In addition, most states have security breach notification laws that apply to certain data.

- **State and federal laws, regulations, case law, and best practices addressing data security.**
  These include federal sector-specific laws such as the Gramm Leach Bliley Act (GLBA) that applies to financial institutions, as well as the HIPAA Security Rule. In general, employers should also consider the meaning of "reasonable security" with regard to BYOD policies.

- **International data protection laws.**
  If a company transfers data between countries, it is important to consider international laws.

- **Legal procedure.**
  State and federal laws that relate to law enforcement access to data and legal procedure and ethics generally. For example, electronic discovery (eDiscovery) is an important issue for employers to consider when creating a BYOD policy.

- **Legal and contractual obligations concerning data retention and secure data destruction.**

- **Confidentiality obligations.**
  These concerns are particularly applicable to the legal, healthcare, and banking industries.

- **Contractual obligations.**
  These might apply to clients or business partners.

- **Trade secret** protection

- **Employment law issues**.
  There are many legal and human resources concerns an employer should address prior to implementing a BYOD policy. A few are listed below.

  - **Wage and Hour** issues under the Fair Labor Standards Act. Nonexempt employees must receive overtime pay
when they work over 40 hours during a workweek. When they have remote access, employees are less likely to
"clock out." Some employers might expect employees to check their emails around the clock, while others may not.

- **Equal Employment Opportunity** [12] laws prohibit employers from discriminating against and harassing employees on
  the basis of race, color, national origin, ancestry, sex, religion, genetic information, pregnancy, age, disability
  (employers must also reasonably accommodate qualified employees with disabilities under the [Americans with
  Disabilities Act](https://www.ada.gov) [13] (ADA)). Laws also require that employers give potential employees equal opportunities.
  Employers must make sure they do not allow BYOD policies to interfere with compliance.
- **Occupational Safety and Health Administration** [14] (OSHA) laws and rules.
- Liability for company access to or loss of personal information on an employee's device.

**B. Security**

**Device loss.** When an employee loses a device he uses for both work and personal purposes (or if someone steals it), the
employer faces a security risk. Many company security breaches result from lost or stolen devices. Company data on an
employee’s personal device can be compromised when he loses the device or the device is stolen.

**Information loss.** Employee error can compromise data and device security [16] as well. Bad habits include using unsecured
wi-fi networks, failing to password protect a device, and allowing the phone to be Bluetooth discoverable. Each of these
increases the risk of an unauthorized person accessing potentially sensitive information.

Malicious software (malware) also threatens device and data security. People can inadvertently download a malicious app, click
on a malicious link, or become the victim of a phishing scam. Some applications, such as peer-to-peer file sharing apps, may
not be malicious per se, but may permit third parties to access data on an employee’s device leaving company data stored there
easily compromised.

Many apps connect a user to data stored "in the cloud." [Cloud services](https://en.wikipedia.org/wiki/Cloud_computing) offer varying degrees of security, so it is important for
employers to know which services employees are using for company purposes.

**C. Protecting data for other business purposes**

Employers must also consider business interests when creating a BYOD policy. These can overlap with legal obligations, or
they may be completely separate.

Employers may be concerned with protecting their reputation or brand integrity. They may also need to protect proprietary
information, trade secrets, or other confidential information. For example, to preserve trade secrets, a company must typically
take adequate steps to protect the information from being disclosed.

**3. What might employees expect to find in BYOD policies?**

BYOD policies (or terms affecting how an employee uses a personal device for company-related purposes) may appear in an
employment contract, orientation materials, employee manual, when an employee decides to use his device, or when the
employee installs an employer’s mobile device management (MDM) software on his/her own device.

*It is important for employees to read an employer's BYOD policy before participating in a BYOD program, and to ask questions.*

Employers must implement policies and company practices to safeguard sensitive information and reduce the risk of legal
liability. In the case of BYOD, the employer should balance this with employee privacy. The following are examples of what an
employee might find in a BYOD policy.

**A. Permitted and prohibited uses, devices, and software**

The policy may state which devices the employer allows to be used for both work and personal purposes. This could also include
acceptable software, brands, and device models.

**B. Employee responsibilities**

An employer may place any number of responsibilities on an employee who is using a device for both work and personal
purposes. Some examples are as follows.

- A company may require an employee to report a lost or stolen device within a certain timeframe.
- Employees may have to account for any time they work remotely.
• The policies should spell out who is responsible for paying for the cost to purchase, replace, service, and repair a device. It will vary by employer, but employees may receive a stipend to purchase a device and be responsible for any additional cost. Alternatively, employees may have to pay for the device but not the service plan. Some employers may require employees to pay for everything, and some hardly anything.
• Employers will likely have exit requirements for employees when they leave the company. These might include deleting data, revoking access to a network, deleting certain apps, etc. Employees may have to turn the device over to the employer to carry out the exit requirements as well.

C. Explanation of available/required technical support

Employers may require employees to work with the employer's IT department to enroll in the BYOD program, receive security updates, agree to remote access to the device, install specific software, and receive continuous support.

D. Consent to certain practices

When an employee receives a copy of the BYOD policy, he or she may have to consent to certain practices. These may include:

Remote data deletion. As a security measure, employers often require employees who store company information on their personal devices to allow the employer to remotely delete data from the phone if the phone is lost or stolen. The same may be true when a person leaves the company.

Employees should ask what data will be wiped from the phone, so that they understand whether or not they risk losing personal photos and videos, downloads, contacts, and anything else that is stored on the device and not backed up elsewhere.

Authorizing access to personal data on a device. When an employee reviews and signs an employer's BYOD policy, she should determine whether the agreement allows the employer to access personal content on the mobile device. Employees should never just assume that their personal content such as emails and applications will remain private.

Requirements to save and produce relevant information for legal purposes (e-discovery in particular) and consequences for deletion or alteration. When an employer is involved in litigation, it will likely need to know where company information resides and what the data consists of. This can be difficult when an employee owns a device and is able to store company data and information in places the company is not aware of.

Who pays for what. An employer may pay for a portion of the personal devices’ cost, the monthly bill, or the data plan. To reduce the risk of unexpected financial responsibilities, employees need to make sure they understand what they are responsible for covering prior to using the personal device for work purposes.

Processes for the end of an employment relationship. In most cases, a company will want to remove its data from an employee's personal device when he or she leaves. The company may require the employee to submit the device to the IT department, or it may just tell the employee to delete the data. Employees will also be disconnected from the network, and no longer able to access it.

Employees should make sure they understand what these processes entail.

Trade secret policies and confidentiality agreements. Employers must protect their trade secrets and proprietary information. If information is valuable and has legal protection because it is secret, an employer must be extremely cautious when allowing employees to handle and transfer information on personal devices and potentially outside the employer's network.

The same is true for businesses with legal and professional duties to maintain confidentiality. Employees must understand their obligations so that they do not accidentally expose sensitive information.

Agree to maintain certain security measures. Employers may require or prohibit specific software on an employee's device.

Employers may require employees to encrypt data stored on the device, and/or require a strong password or other security measures to access the device. They may also ask for the ability to remotely locate the device, and automatically wipe the device of all data in certain instances (too many incorrect password attempts, for instance).

E. Explanation of mobile device management software

Employers may use mobile device management software (MDM) to exercise control over the devices employees use for both personal and work-purposes. MDM software may enable the personal device to access the employer’s network or cloud with added security. It may be used to remotely wipe a device if the individual loses it or it is stolen, or to prevent personal apps from
accessing company information. MDM software can prohibit a user from installing certain apps and require a device to update apps. Employers may also use it to set other security protections.

Using a personal device on an employer’s network may allow the employer to access the information, even personal nonwork-related information, contained on your personal device.

4. Why are employees concerned about their privacy?

Most people carry their personal devices, especially smartphones, with them wherever they go. For some, using personal devices for work is a convenience that helps them multi-task. Others find that their personal and work lives blend more than they would like.

Employees may be unhappy when an employer has any control at all over how they use their personal device. Many don't trust employers with their personal data, and further distrust them with keeping it private and not using it against them.

What if an employee uses a mobile health app to monitor a medical condition, and she does not want her employer to know? How private are personal email accounts, photos, calendars, etc.? If an employer does not manage employees’ expectations or adequately disclose what it does and does not do, employees have reason to be concerned about their personal privacy.

So what can employers do with this access to an employee’s personal device? There is a difference between what a particular employer can do and what an employer actually will do. The following is a non-exhaustive list of what is possible (but will completely depend on the employer, agreement, and software):

- Locking, disabling and data wiping – the employer may have retained the right to remotely lock or disable the employee’s personal device or delete any and all data contained on the phone.
- Access to the device
- Access to phone records or contacts
- Access to social media or other account username and passwords
- Monitor GPS and location information
- View Web browsing history
- View pictures, video, or other media
- View personal emails
- View chat and messaging histories
- Limit the use of cloud services

BYOD policy terms, even if present, may or may not indicate when or how often the employer will actually do any of these things. It may also include vague language that can leave an employee unsure under what circumstances the employer will access the personal device and what added responsibilities an employee takes on.

5. Tips for employees considering participating in a BYOD program

A. How employees can protect their privacy proactively

- Think carefully about whether to use a personal electronic device for work purposes at all. Employees should read their employer’s BYOD policy thoroughly. Be aware that these policies often use legal and technical jargon that may be difficult to understand. For this reason, employees may decide they want to speak with an attorney, or at least clarify their concerns with the HR department. Consider whether any potential privacy compromises are worth taking on in order to use a personal device at work. Not participating in BYOD is the best way to keep the private information on a personal device private, but it might be less convenient.

- Determine whether it is feasible to have two separate personal devices – one purely for work purposes and one for everything else. An employee who wants to use a personal device for work purposes may decide to have a separate device solely for work. This option can be extremely costly (especially if the employer is not covering the plan), but separating personal activity from work activity on individual devices significantly limits the personal information available to the employer. People with an older device they no longer use may want to completely clear it of personal information and convert it to a “work only” device.

- Before participating, all employees should read and understand the employer’s BYOD policy. Ask questions. Employees should educate themselves about what they are agreeing to when participating in a BYOD program at work. With respect to employee privacy, understand when the employer may access a device or monitor its use.
Employees who participate in BYOD programs should be conscious of privacy settings, information they store on their device, and apps they use. Mobile device owners should familiarize themselves with any settings that impact privacy or security. These include (but are not limited to) Bluetooth sharing, automatically connecting to wi-fi networks, location-based services, and available security settings. Also, consider restricting others from using the device, and password protecting certain apps or functionalities on the device.

Employees should back up important personal data stored on their devices such as photos, videos, music, etc. It is always a good idea to back up important data. However, employees who participate in a BYOD program have added incentive to back up personal data if the company has the ability to remotely wipe data from a device.

If an employee is concerned about an employer accessing certain personal data, she/he may also want to periodically delete data from the device and transfer it somewhere more private.

**Consider situations that may arise down the road from participating in an employer’s BYOD policy.** It's impossible to predict the future, but employees should weigh the potential costs and benefits of BYOD programs.

- If the employer becomes involved in litigation or an investigation, certain employees may be required to turn over a personal device if it contains relevant data. If this happens, to what extent are the personal contents of the device available for others to see?
- When an employer uses a data backup system, could personal information be backed up and saved as well? Can an employer access this?
- Agreeing to a BYOD policy may reduce an employee's reasonable expectation of privacy under the Fourth Amendment. Agreeing to an employer's BYOD policy may affect the extent to which the Fourth Amendment protects an employee from law enforcement searches and seizures of the device. Fourth Amendment protections apply only when an individual has a reasonable expectation of privacy in the place (in this case the device) being searched. However, when an employee agrees to a BYOD policy permitting an employer to access his device, he could lose his expectation of privacy.
- BYOD policies may result in unclear performance evaluation standards. For example, is the employee expected to respond to emails after hours?

These are only a few situations to consider, and the law surrounding BYOD is evolving. Every employment situation and policy will be unique.

**B. When employees believe an employer has violated their privacy**

In the area of employment law, the facts are very important and state laws vary. With regard to BYOD policies, the law is emerging as more employees use mobile devices for both work and personal purposes. This means legal issues are less likely to have clear cut answers. Issues and policies will also depend on the specific employer. Government employees, employees of private companies, and employees in highly regulated industries should have different expectations.

Employees should discuss legal concerns with an attorney. However, it is probably most important for employees to understand their employer's BYOD policy before agreeing to it.

The following are just some of the issues an employee may encounter and want to discuss with an employment attorney.

- An employee believes the employer accessed personal content without the employee's consent during or after employment. This can be a tricky issue, but the best way to avoid it is to understand the employer's BYOD policy before adopting it. Just a few considerations are listed below:
  - The Stored Communications Act [19] (SCA) may be relevant depending on the facts.
  - Privacy tort law may apply to a situation, but will depend on the state and heavily on the facts.
  - Certain states have enacted laws [20] that prevent an employer from requesting or requiring access to an employee's social media accounts. In many others, legislation has been introduced or is pending.
  - Protections may apply to an employee's privileged communications with his/her attorney.
  - An employee may believe he/she is being harassed in the workplace by coworkers or superiors as a result of blurred boundaries between personal and work matters.
  - An employee is concerned he/she is not being compensated appropriately for remote work. For example, a nonexempt worker may put in overtime as a result of having work readily accessible on a personal device.
An employee believes he/she is being discriminated against because of personal content an employer accesses on a device he/she uses for both work and personal purposes. For example, an employee may have an app that monitors a health condition or relates to a disability.

An employee believes he/she has incurred a cost relating to the device or plan that the employer should have paid.

6. Tips for employers implementing a BYOD program

- **Develop a policy.** If possible, create an internal BYOD policy before allowing employees to use devices for both work and personal purposes.

- **Balance risks with fairness to employees.** When developing the policy, take employee expectations into account and make sure the policy is practical.

- **Where different employee roles handle different data, develop policies specific to a job function/role.** Policies/practices/security controls/access should vary according to an employee’s role and job function. A successful BYOD program will account for risks based on the employee’s role and access to information.

- **Raise employee awareness.** Explain the policy and offer periodic training for employees. Encourage employees to ask questions, and address potential tradeoffs. Employee education efforts are crucial to a successful BYOD program.

- **Encourage employees to ask questions.** If employees understand the policy they are less likely to violate it. They are also less likely to put the employer at risk, believe their privacy is being violated, and engage the employer in litigation down the road.

- **Provide employees with the tools they need to implement the policy.** For example, if the BYOD policy requires an employee to use specific security software, the employer should provide it.

- **Revisit the BYOD policy on a regular basis.**

7. Additional resources

- **National Employment Lawyers Association Directory** [21]
- **National Labor Relations Board** [15]
- **U.S. Equal Employment Opportunity Commission** [12]
- **U.S. Department of Labor: Wage and Hour Division** [11]

**Relevant Articles and Guides by Law Firms**


**Privacy Rights Clearinghouse Fact Sheets:**

- **Fact Sheet 2b: Privacy in the Age of the Smartphone** [24]
- **Fact Sheet 7: Workplace Privacy and Employee Monitoring** [25]
- **Fact Sheet 18: Online Privacy: Using the Internet Safely** [26]
- **Fact Sheet 36: Securing Your Computer to Maintain Your Privacy** [16]

Source URL (modified on September 22, 2016): https://www.privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk

Links