

# PRIVACY LAW

Analysis of Privacy Law

Jesse Russell

Eastern Michigan University

### Analysis of Privacy Law

Most of us are familiar with the fact that the U.S. Constitution, along with Bill of Rights, provides safeguards to protect the American people from tyrannical governments and keeps the United States Government from overstepping their boundaries. Among these is the right to privacy, discussed in Amendment IV of the constitution. In this amendment, the groundwork is laid out to protect American citizens from unreasonable search and seizure from any government entity. This includes police officers, judges, courts, and any other governmental employee. How does this apply when the private sector is involved? This paper will analyze the legality of private search and seizure by companies in the private sector regarding the employees of that company, through 3 hypothetical situations.

In the first hypothetical, we have a private company based in Ypsilanti, Michigan that would like the ability to monitor the computers of the employees, place MDM software on the employees' phones, search lockers, and vehicles on company grounds. The fourth amendment of the constitution only applies to governmental entities, and the private sector is excluded from this (with exception that will be discussed in a later section). (U.S. Const. Amend. IV) However, this does not mean that the company has the ability to search its employees at any time, for any reason. The employees must be subject to a reasonable expectation of privacy, similar to the fourth amendment, but the employer has the right to reduce the expectation of privacy through clear policy stating that employees are subject to search. The company must also have a reasonable justification for the search, such as if management receives a tip that there may be a weapon in the employee's locker, and he intends to use it to harm his coworkers. The policy for this company should read: "If any employee of [insert company name] is suspected of intent to harm individuals; possess/distribute illegal contraband (such as drugs, alcohol, weapons, etc);

violate company policy; participate in any illegal activity (federal or state); or possess/distribute pornography involving minors, management may conduct a search into that employee's locker, vehicle, desk, computer, and communications, on company property. Should management find any contraband, incriminating evidence, or policy violation, that evidence may be surrendered to authorities and/or the employee may be terminated." This wording explicitly states the policy regarding private search and seizure, so the employee's reasonable expectation of privacy is limited.

There is an exception to the fourth amendment, though. It does not apply to the private sector, unless that company is contracted by the US government, and ordered to conduct searches of its employees. In the second hypothetical, a private sector company in Sandusky, Ohio is recruited by the US government to create two-way radios for the military and government. The government directs the company to conduct searches of its employees coming into work, as well as in their homes and families. Even though this company is in the private sector, it is contracted by the government, so this would be a direct violation of the employees' fourth amendment right. In *United States v. Kennedy* (2000), the court concluded that there if no government agent is involved in a search, the search is not a violation of the fourth amendment. Inversely, if this hypothetical company were to conduct searches on the behalf of the US government, this would be a violation because it would now be a government action instead of a private one. The policy for this company should read: "[Insert company name] cannot conduct unreasonable searches on its employees ordered by the US government without a warrant, as this would be a violation of the fourth amendment to the constitution of the United States. The company does, however, reserve the right to conduct a private search on company grounds on a reasonable suspicion of illegal activity, company policy violation, possession of illegal contraband, child pornography,

and any other incriminating offense; so long as it is not conducted or ordered by a government entity. If this private search yields evidence of illegal activity, this evidence may be turned over to the proper authorities, and the employee may be terminated.”

For the third hypothetical, let’s take the conversation overseas. A company based in Paris, France wants to collect data on consumers around the world, based on databases, searching websites, and deploying hidden computer code to computers that visit websites for commerce. According to the General Data Protection Regulation (GDPR) (2016), data controllers must keep privacy in mind when designing data systems. This regulation is designed to give citizens of the EU control of their personal information. Under this, the company would not be able to harvest data using these methods, as the GDPR clearly specifies what data must be used for. If a company is found negligent of handling user data, they may be fined up to €20 million. This regulation is similar to or fourth amendment, but it applies to all parties involved, including the private sector. This company’s policy on the information should read: “[Insert company name] cannot harvest data without disclosing precisely how that data will be handled, and must have reasonable measures in place to protect from data breaches. The company must also report any data breach within 72 hours, in order to protect the company from fines. The mining of data must comply with the General Data Protection Act of 2016 in all instances.”

To conclude, it is our duty to know our constitutional rights and understand how to render a solution if those rights are infringed. As a public company, we must do everything in our power to follow the constitutional rights appointed to our citizens so that we do not open ourselves to litigation.

References

U.S. Const. amend. IV

United States v. Kennedy, 81 F. Supp. 2d 1103, 1112 (D. Kan. 2000)

Regulation 2016/679. General Data Protection Regulation. European Parliament, Council of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>