December
2023

PRIVACY & CIVIL LIBERTIES CASE LAW EXAMPLES

JOB AID

CDSE Center for Development of Security Excellence

Privacy and civil liberties are an important component of a multidisciplinary insider threat program because there is a responsibility to safeguard constitutional rights while carrying out the duties of an insider threat program. Insider threat program personnel may have access to a diverse range of information as part of their duties. Ensuring that this information is handled properly is paramount, particularly if the information is to be referred to and used by law enforcement agencies in their investigations. Insider threat professionals must understand privacy and civil liberties and seek advice from privacy and civil liberties professionals who can provide expertise regarding legal implications.

The U.S. Constitution and its amendments, laws passed by the U.S. Congress, or laws signed by the president are all important to an insider threat program. The three primary amendments that may be involved in insider threat cases are the First Amendment, Fourth Amendment, and the Fifth Amendment. Since safeguarding individual constitutional rights may be at stake, insider threat program professionals must confer with their agency privacy and civil liberties or legal sections. Additionally, insider threat program professionals must confer with human resources and senior management, as they are intricately involved in employee matters and personnel policy decisions.

The **First Amendment** of the U.S. Constitution reads that "Congress shall make no law, respecting an establishment of religion, or prohibiting exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people to peaceably assemble, and to petition the Government for redress of grievances."

The **Fourth Amendment** of the U.S. Constitution protects people from unreasonable searches and seizures by the government. The Fourth Amendment, however, is not a guarantee against all searches and seizures but only those that are deemed unreasonable under the law.

The **Fifth Amendment** of the U.S. Constitution cites that "no person…shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." This amendment is best known for cases in which someone invokes the Fifth when testifying.

Notable cases that focus on the First, Fourth, and Fifth Amendments of the U.S. Constitution are summarized in the following pages.

FIRST AMENDMENT CASES

Garcetti v. Ceballos
547 U.S. 410 (2006)

Is a public official's speech protected by the First Amendment only in a private context or does it also apply during the exercise of official duties? In this case, a sheriff in the Los Angeles District Attorney's office misrepresented facts in a search warrant affidavit. When Richard Ceballos, who worked in the office, discovered the misrepresentation, he told the prosecutors who were working on the case. They refused to dismiss the case, even though they agreed that the affidavit was dubious.

Ceballos took his information to the defense counsel, who subpoenaed him to testify. He later brought a claim against his employer on the grounds that he had suffered from retaliation for cooperating with the defense, which he argued was protected by the First Amendment. The trial court ruled that qualified immunity protected the district attorneys, but the Ninth Circuit found that it did not apply because Ceballos had been engaging in activity covered by the First Amendment protections on speech regarding matters of public concern.

In a 5-4 majority opinion, the U.S. Supreme Court ruled that public employees are not considered to be speaking as citizens for First Amendment purposes if they are making statements pursuant to their official duties. The First Amendment does not protect them from discipline by their employers. In this case, the employee properly received discipline because of his cooperation with the defense, which undermined his ability to carry out his official duties.

An insider threat program may have to consider statements made by individuals as to whether they meet the thresholds of insider threat reporting or if they are protected under the First Amendment of the U.S. Constitution.

New York Times Co. v. United States ("The Pentagon Papers" Case)
403 U.S. (1971)

Can the government prevent the publication of classified information even if that information is vital to protecting national security? The *New York Times* and the *Washington Post* both gained access to the so-called "Pentagon Papers" – a classified Department of Defense study that examined the history of U.S. involvement in Vietnam.

Daniel Ellsburg was employed at the RAND Corporation and worked on the report. He photographed thousands of pages and sent it to a *New York Times* reporter. In 1971, the *Times* began publishing it. The Nixon administration argued that these news reports endangered national security and went to court to try to block the continued publication of the Pentagon Papers.

In a *per curiam* decision (meaning one written "by the court as a whole"), the Supreme Court rejected the Nixon administration's efforts, concluding that they could not overcome the "heavy presumption against" prior restraints or efforts by the government to block others from publishing information in the first place. In America, there is a long tradition, extending back to the founding generation, opposing these kinds of limits on the freedom of the press. As a result, the newspapers could continue to print the Pentagon Papers.

The Pentagon Papers case reaffirmed a value at the core of the First Amendment – the freedom of the press to criticize the government and check abuses of power. While this case illustrates the freedom of the press, it further illustrates the potential damage an unauthorized disclosure can cause because once information is provided to the press, it is then protected, which could allow its release to the public. Insider threat programs endeavor to identify potential insider threats and risks before the information is released and the damage is done.

FOURTH AMENDMENT CASES

O'Connor v. Ortega
480 U.S. 709 (1987)

Does an employee have an expectation of privacy in their workplace? In this July 1981 case, Dr. Dennis O'Connor, director of Napa State Hospital, became concerned about allegations of misconduct against Dr. Magno Ortega. While Dr. Ortega went on leave, a team within the hospital entered Ortega's office "to secure state property." They searched the office thoroughly and seized several items that were later used in his hearing to impeach a witness. They also seized papers relating to private patients.

Dr. Ortega was later terminated, and he took his former employer to court. The lower courts held that the search violated Dr. Ortega's right to privacy. The Supreme Court, however, stated that Ortega's rights were violated "only if the conduct of the hospital officials at issue in this case infringed an expectation of privacy that society is prepared to consider reasonable." The Court outlined the areas related to work that are within an employer's control and stated those areas are the province of the employer, even though an employee may be allowed to place personal items there. This would not extend to closed luggage, such as handbags and briefcases, however.

The Court also stated that employees may expect privacy against intrusions by law enforcement but that employees never have a reasonable expectation of total privacy in their place of work when supervisors are involved. As in this case, employees may possess, acquire, or report information of concern, and this information may be within the employee's workspace or on a work device. Insider threat programs must be cognizant of how information is obtained and whether it violates an employee's reasonable expectation of privacy and Fourth Amendment rights.

Thygeson v. U.S. Bancorp
2004 WL 2066746 (D. Or. 2004)

Can an organization's policies prohibit the use of their computers to access inappropriate sites or to send emails perceived as inappropriate or offensive? In this case, Phil Thygeson was a regional manager for U.S. Bancorp Equipment and Finance, Inc., which had established policies doing just that – prohibiting the use of their computers to access inappropriate sites or to send emails that were perceived as offensive. If employees did so, they could be subjected to disciplinary action, including termination. Thygeson accessed the internet to view inappropriate content, including sexually explicit cartoons and images of adults, and emailed them to others, including subordinate employees.

Thygeson was terminated for cause for violating the company's code of ethics and conduct on the job. He then filed a legal claim against his employer. The Supreme Court ruled against Thygenson, citing his failure to prove the essential elements of liability under 29 U.S. Code Section 1140, in that he did not have a reasonable expectation of privacy on the explicit internet websites. He accessed those websites from his computer even though employees were informed of the acceptable use policy and that the company could monitor and access employee emails. Employees were also aware that they could be subject to disciplinary action, including termination, if found in violation of those policies.

This case illustrates the importance of an insider threat program team working closely with management, human resources, and information technology so they are fully aware of how information is obtained and reported to an insider threat program and what information can be accessed for its purposes.

FIFTH AMENDMENT CASE

Garrity v. New Jersey
385 U.S. 493 (1967)

Can public employees be compelled to incriminate themselves during investigatory interviews conducted by their employers? The case of *Garrity v. New Jersey* addressed this.

In 1961, the New Jersey Attorney General began investigating allegations that traffic tickets were being "fixed" in the townships of Bellmawr and Barrington. The investigation focused on Bellmawr police chief Edward Garrity and five other employees. When questioned, each was warned that anything they said might be used against them in a criminal proceeding and that they could refuse to answer questions to avoid self-incrimination. However, they were also told that if they refused to answer, they would be terminated. Rather than lose their jobs, they answered the investigators' questions. Their statements were then used in their prosecutions over their objections, and they were convicted.

In 1967, the Supreme Court ruled that employees' statements made under threat of termination were compelled by the state in violation of the Fifth and Fourteenth Amendments. The decision asserted that "the option to lose their means of livelihood or pay the penalty of self-incrimination is the antithesis of free choice to speak or to remain silent." Therefore, because the employees' statements were compelled, it was unconstitutional to use the statements in a prosecution. Their convictions were overturned.

Insider threat programs may encounter situations where they may need to talk to employees to gather information. They must be cognizant that employee information must be willingly obtained whether they obtain it or if it were obtained from outside the insider threat program.

ADDITIONAL RESOURCES

Insider threat professionals can learn more about privacy and civil liberties and obtain more detail relating to these and other cases from the following sources:

U.S. Department of Justice, Office of Privacy and Civil Liberties

U.S. Department of Justice Bureau of Justice Assistance

U.S. Department of Homeland Security

United States Courts

U.S. Department of Defense Privacy, Civil Liberties, and Freedom of Information Directorate

U.S. Department of Defense Counterintelligence and Security Agency

Public Access to Court Electronic Records

NOTE: If the URLs in this document do not open upon clicking, right-click on the hyperlinked text, copy link location, and paste into a browser. Alternatively, you can open the PDF in a browser.