CRJS475 Unit 3 Individual Project – Constitutional Requirements for Digital Searches and Seizures

Framers of the Constitution on Digital Searches and Seizures

Cell phones, computers, and digital devices have become universal because they keep people connected to the world and to each other. Digital devices contain huge amounts of personal information, and they have password protection to safeguard privacy. However, if someone has been arrested and charged with a crime, then the contents of the digital device may become an issue (Khonsari, 2019). What are the constitutional digital privacy rights of someone when law enforcement wants to search the contents of their digital devices?

The framers of the Constitution could not have imagined the digital world of today. However, their specific language from 1791 continues to protect important constitutional rights. Even though cell phones did not exist when the Fourth Amendment was written, it still prohibits law enforcement officers from unlawfully seizing and searching those digital devices (Khonsari, 2019). Digital searches and seizures must be done lawfully by adhering to Fourth Amendment restrictions.

Today's courts have noted that digital data can provide a comprehensive, detailed, and intrusive overview of the private affairs of people's lives. For example, the Court has noted the following:

> Few [people from the 1700s when the Constitution was written] could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements. (Travieso & Lyon, 2019)

The Court stated that a cell phone is almost an extension of the human body, much like an arm or a leg, because it tracks almost all of the movements of its owners, who are "compulsively" carrying their cell phones everywhere, including doctor's offices, political headquarters, friends' homes, and so on. (Oyez, n.d.b; Travieso & Lyon, 2019).

Fourth Amendment and Digital Protections

Under the Fourth Amendment of the Bill of Rights, people are protected from unlawful searches and seizures by the government. They have the right to be secure in their "persons, houses, papers and effects, against unreasonable searches and seizures" (Khonsari, 2019). The Fourth Amendment recognizes that information (including cell phone, computer, or digital data) is protected by the Constitution. For example, in *Riley v. California* (2014), the Court unanimously required a warrant to search a phone that was seized during an arrest (Shapiro, 2017). The Fourth Amendment to the U.S.

Constitution protects people from unreasonable or illegal searches and seizures by government officers, and that protection extends to cell phones, computers, and other digital devices (Fakhoury & Kayyali, 2014).

Court Order to Track Cellphones

Under the Stored Communications Act (codified at 18 U.S.C. Chapter 121), prosecutors must obtain a court order to track, monitor, or eavesdrop on digital data from cell phones and other electronic devices from suspects. Prosecutors must demonstrate that there are "specific and articulable facts showing that there are reasonable grounds to believe" that the records are "relevant and material to an ongoing criminal investigation" (Travieso & Lyon, 2019).

Warrants and Digital Searches

After a person has been arrested, the police generally conduct a warrantless search of the items on their person, as well as anything within their immediate control, such as anything that is within lunging distance from them. However, the U.S. Supreme Court has ruled that law enforcement cannot search the digital data that are stored on a cell phone unless a warrant is obtained to do so (Fakhoury & Kayyali, 2014). However, a warrantless search may be conducted of a digital device in the following situations:

- The subject provides a consent to search.
- Officers have probable cause to believe that incriminating evidence on a phone is under immediate threat of destruction, such as an exigent circumstance (Khonsari, 2019). In situations where law enforcement believes that evidence on the phone is likely to be immediately destroyed, then officers can search the cell phone without a warrant (Fakhoury & Kayyali, 2014).

When an officer arrests someone, the arrestee may refuse a warrantless consent to search their digital devices (e.g., cell phones, computers, and so on). In a warrantless situation, officers may only conduct an exterior physical search of a cell phone, such as removing the case or the battery because that is not an invasive interior search for digital data (Khonsari, 2019).

Generally, to search a digital device, officers need to apply for a warrant by presenting probable cause to a judge to justify a search and seizure. *Probable cause* means that there is a "certain level of suspicion of criminal activity" (Khonsari, 2019). If an officer is applying for a warrant to conduct a digital search, then the warrant application should contain the following:

- The name of the person arrested or the exact address and the specific places to be searched
- A list of the items that can be seized or taken by the police
- A judge's signature that authorizes the search
- A deadline or date for when the arrest or search must take place (Search warrants do not last indefinitely, and they must be executed within a specific time line.)

Officers must take the search warrant with them to execute it and give the person or the defendant a copy of it. A warrant may do the following (Fakhoury & Kayyali, 2014):

- Allow officers to seize digital devices and computers and take them away to another location to enable forensic experts to conduct more thorough searches
- Make a copy of data, media, files, or other information that is stored on a computer or a digital device

Illegal Digital Searches: Fruit of the Poisonous Tree Doctrine

> It is better to let ten guilty people go free, than to convict one innocent person. – William Blackstone (1765)

The *exclusionary rule* prevents officers from using illegally obtained evidence against a defendant in court (Khonsari, 2019). If an officer illegally searches a digital device, then they have violated the constitutional rights of someone, and the evidence that is obtained from the search is dismissed from criminal proceedings (Fakhoury & Kayyali, 2014). The exclusionary rule comes from the fruit of the poisonous tree doctrine. An illegal search is a poisonous fruit that harms the constitutional rights of people—innocent or otherwise. There are some good faith exceptions to the exclusionary rule, but they are not discussed in this course.

Fifth Amendment and Digital Protections

Officers can ask people or arrestees to voluntary provide passwords or encryption keys to digital devices, but they are not required to surrender them. It falls under the Fifth Amendment Miranda privilege, where they are not required to provide incriminating evidence against themselves.

> You have a right to remain silent – and anything you say can and will be used against you in a court of law.

The *Fifth Amendment* protects people from being forced to give the government self-incriminating testimony. Courts have generally accepted that telling the government a password or encryption key is testimony. As a result, an officer cannot compel or threaten someone into giving up their password to unlock an electronic device (Fakhoury & Kayyali, 2014).

If officers do not have a warrant, they can still ask roommates, spouses, or partners for passwords to gain access to someone's digital devices. The rules governing exactly who can consent to a digital search are still somewhat gray. The legal key is to determine who has legal control over a digital item. For example, consider the following (Fakhoury & Kayyali, 2014):

- If a spouse with physical control of a digital device grants consent to search, then officers may conduct a legal search.
- Conversely, if the other spouse with digital control denies consent to search, then officers may not search.

Another similar gray issue that may arise is a shared computer that is in a living room that is used by roommates. Officers must determine who has legitimate control and access to the computer. For example, does a third party have the legal right to provide a consent to search? Many of these legal issues continue to evolve in the court system in the 21st century.

Third-Party Doctrine Explained

The *third-party doctrine* is applicable to situations where evidence is in the possession of a third party, such as the following (Travieso & Lyon, 2019):

- Cell phone or wireless companies
- Cloud service providers, such as e-mails, file hosting and sharing services, and so on
- Banks, stores, corporations, and so on
- An individual person, such as spouses, friends, roommates, and so on

The legal question that arises for the government is as follows:

> What evidence collection mechanism will be used, and does it impact or violate the Fourth Amendment?

When officers collect digital records of people via a third party, it affects their Fourth Amendment constitutional protections (Travieso & Lyon, 2019).

Carpenter v. United States and Third-Party Searches

Third-party cell phone technology can provide investigators with the ability to track down the past and present locations of any person who carries a cellphone. It can also track the following:

- Locations where the cell phone holder visited
- The number of times that they were there and how long they stayed
- Other cell phones that were present
- Who associates with whom
- Digital connections between people in a community, nation, or criminal enterprise

The aforementioned can be instrumental information for building and prosecuting criminal cases. However, the U.S. Supreme Court ruled in 2018 in the *Carpenter v. United States* case that law enforcement needs a warrant to search or track cell phone data. The *Carpenter v. United States* case addressed third-party issues, which means that if someone shares information with a third party, then

they have a reduced expectation of privacy but still have a legal expectation of privacy. For example, the third party in the *Carpenter* case was a cell phone company. The Court ruled that in that case, a warrant is needed to obtain a defendant's location when using third-party cell phone towers for tracking locations (Khonsari, 2019).

Carpenter v. United States Case Explained

Timothy Carpenter and Timothy Sanders were convicted of charges stemming from a string of armed robberies. They appealed on the grounds that the government illegally acquired third-party cell phone records without a warrant, which showed their physical movements around the city, which is a violation of the Fourth Amendment. The U.S. Supreme Court subsequently overturned their conviction because the warrantless digital data were illegally obtained. The defendants had a contract with the phone company, and their data should not have been released to the government without a warrant. In that particular case, the following circumstances were true (Shapiro, 2017):

- Law enforcement did not have an exigent circumstance that threatened the destruction of cellphone data.
- There was no threat to officer safety.
- Officers could have easily applied for a warrant, but they did not.

The government illegally used the third-party doctrine to circumvent the requirement for obtaining a warrant. The government incorrectly argued the following:

> Once a cellphone user signs a contract with a cellphone company, then he [allegedly] forfeits his Constitutional Fourth Amendment expectation of privacy – because the third-party information does not belong to him, but it belongs exclusively to the cellphone company. (Travieso & Lyon, 2019)

However, when a third party is acting under the color of authority for a governmental request, then the government is still required to get a warrant. Specifically, using a third party does not exempt the government from Fourth Amendment search and seizure requirements.

Warrantless Digital Searches at U.S. Borders

There is a reduced expectation of Fourth Amendment digital privacy when a person crosses a U.S. border. Officers may conduct warrantless searches of computers and other digital devices at U.S. borders, even if there is no suspicion of anything illegal. An international airport that is several miles away from the actual border is still considered the functional equivalent of a U.S. border for warrantless searches of digital devices (Fakhoury & Kayyali, 2014).

Conclusion

Cell phones, computers, and digital technology did not exist when the Constitution was originally written. However, the underlying principles of constitutional safeguards are embedded in the text of the Fourth Amendment, and those principles must be applied to 21st-century technology. The Fourth Amendment was ratified in 1791, and then the *Carpenter v. United States* case used that same Amendment to settle a legal digital dispute 227 years later in 2018. Constitutional issues for digital searches and seizures will continue to evolve in the legal system over the next century.

References

Blackstone, W. (1765). *Commentaries on the laws of England* (1st ed.). Clarendon Press at Oxford.

Cornell Law School. (n.d.a). *Consent searches*. https://www.law.cornell.edu/constitution-conan/amendment-4/consent-searches

Cornell Law School. (n.d.b). *18 U.S. Code Chapter 121—Stored wire and electronic communications and transactional records access*. https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

Cornell Law School. (n.d.c). *Exclusionary rule*. https://www.law.cornell.edu/wex/exclusionary_rule

Cornell Law School. (n.d.d). *Exigent circumstances*. https://www.law.cornell.edu/wex/exigent_circumstances

Cornell Law School. (n.d.e). *Fruit of the poisonous tree*. https://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree

Cornell Law School. (n.d.f). *Good faith exception to exclusionary rule*. https://www.law.cornell.edu/wex/good_faith_exception_to_exclusionary_rule

Fakhoury, H., & Kayyali, D. (2014, October). *Know your rights*. Electronic Frontier Foundation. https://www.eff.org/issues/know-your-rights

Khonsari, R. (2019, May 9). *Cell phone privacy rights: What you need to know*. Khonsari Law Group. https://klgflorida.com/cell-phone-privacy-rights/

Oyez. (n.d.a). *Carpenter v. United States*. https://www.oyez.org/cases/2017/16-402

Oyez. (n.d.b). *Riley v. California.* https://www.oyez.org/cases/2013/13-132

Shapiro, I. (2017, August 13). *To apply the Fourth Amendment in the digital age, go back to its text*. CATO Institute. https://www.cato.org/blog/apply-fourth-amendment-digital-age-go-back-its-text

Travieso, F., & Lyon, E. M. (2019, January 15). *The legal implications of digital privacy*. GovTech. https://www.govtech.com/public-safety/the-legal-implications-of-digital-privacy.html

U.S. Department of Justice (DoJ). (n.d.). *Deprivation of rights under color of law*. https://www.justice.gov/crt/deprivation-rights-under-color-law