October 1, 2018

Rennehan,Richard

isec3050-701

Third-Party Doctrine

Assignment 1

Contents

[Introduction 2](#_Toc526195011)

[Brief History of the Fourth Amendment and Third-Party Doctrine 3](#_Toc526195012)

[Does the Third-Party Doctrine Conflict with the Fourth Amendment? 5](#_Toc526195013)

[Where Does 21st-Century Data Fit in? 7](#_Toc526195014)

[Conclusion 9](#_Toc526195015)

[References 10](#_Toc526195016)

# Introduction

Does the Third-Party Doctrine conflict with the Fourth Amendment? What’s happening with our 21st-century data? With the rise of an economy based on the data of the people, many such questions have been raised. Our goal is to balance data collection and protection, so our technological lives can be easier and more efficient while still protecting our data from unreasonable searches. If we take too much action at once, however, the economy will take a heavy blow and many businesses may go out of business.

This document will explain the possible outcomes for the future by looking at a history of related case outcomes and events.

# Brief History of the Fourth Amendment and Third-Party Doctrine

The Fourth Amendment was approved on December 15, 1791. It was created to protect people against unreasonable searches and seizures in their homes and property. For police to conduct a search, a warrant or a probable cause was required. This was a time where most property belonging to someone was physical. As time passed, a shift towards personal data and information raised the question on whether intangible property should be protected as well (Ronald McLeod, 2018).

In a 1928 case, the government requested a phone company to tap the phone line of Roy Olmstead to record his conversations, all without a warrant. Although the tapping resulted in evidence of him bootlegging, Roy Olmstead fought to exclude the evidence, stating it was an unreasonable search. The issue was settled in Supreme Court. He argued that monitoring phone calls without permission or warrant was an example of unlawful search and seizure. The court found he was not protected under the Fourth Amendment because the police were not in his home, therefore not a search and seizure (*Olmstead v. United States*, 1928).

This decision would be overturned in the *Katz v United States* (1967) case. The primary holding was, according to the contributions of Chris Skelton (n.d.), “It is unconstitutional under the Fourth Amendment to conduct a search and seizure without a warrant anywhere that a person has a reasonable expectation of privacy, unless certain exceptions apply”. This means the Fourth Amendment now covers intangible property as well (para. 1).

However, in the late 1970s, a new legal principle developed, called the Third-Party Doctrine. It says if you engage in a contract with a third party and share information about yourself, they have the right to do anything they please with it. It assumes you have no reasonable expectation of privacy for any information you voluntarily hand over. (Ronald McLeod, 2018).

The Third-Party Doctrine was in its infancy back in March 1976 where a Baltimore woman was robbed and reported details of the robber to the police. Not long afterward, she began to receive threatening phone calls from a man identifying as the robber. Without seeking a warrant, the police asked a phone company to install a pen register to create a record of all numbers dialed by the man. It was determined the caller was the robber and was taken to court. He argued that the evidence from the pen register should be excluded. He felt the use of it without a warrant violated his Fourth Amendment rights against unreasonable searches and seizures. It was eventually raised to the Maryland Supreme Court under the case name, *Smith v. Maryland*. The court agree that if you voluntarily share your information to a third-party, you have “no legitimate expectation of privacy” over that information. (John Villasenor, 2013, para. 5*)*. This brought to life the Third-Party Doctrine (Ronald McLeod, 2018).

# Does the Third-Party Doctrine Conflict with the Fourth Amendment?

Before the data age, it is safe to say that the Third-Party Doctrine and Fourth Amendment co-existed peacefully. However, the areas which they conflict increase with the introduction of new technology and law. This section will compare the fundamentals behind each, give examples, and explain how they are becoming more conflicted over time.

Let’s start by comparing the fundamental values of the Fourth Amendment and Third-Party Doctrine Reflecting to the Katz v. United States case, Chris Skelton (n.d.) summarizes, “It is unconstitutional under the Fourth Amendment to conduct a search and seizure without a warrant anywhere that a person has a reasonable expectation of privacy, unless certain exceptions apply.” (Katz v. United States, 389 U.S. 347 (1967)). For the Smith v. Maryland case. David S. Kemp (n.d.) summarizes, “The installation and use of a pen register, which is an electronic device that records all numbers called from a particular telephone line, by police does not constitute a violation of the ‘legitimate expectation of privacy’ under the Fourth Amendment of the U.S. Constitution because the numbers would be available to and recorded by the phone company anyway” (para. 1).

The common link is the expectation of privacy. If the person has a reasonable expectation of privacy, the Fourth Amendment applies. If the person’s expectation of privacy is unreasonable, the Fourth Amendment doesn’t apply. When you sign with a company, you are consenting them to use your information in the ways described on the agreement. Therefore, expecting privacy on that information today is typically unreasonable, providing the company followed their share of the agreement. However, if the company unlawfully shared information or did something that failed to follow the agreed privacy contract, you would have a reasonable expectation of privacy over the information affected and the evidence should be thrown out.

Exceptions are beginning to apply as of recent. Many believe sensitive information should be recently, a court case, *Carpenter v. United States*, resulted in a momentous decision: that “the government generally needs a warrant if it wants to track an individual’s location through cell phone records over an extended period of time” (Ariane de Vogue and Clare Foran, 2018, Para. 1). With tracking data protected, other information of a sensitive nature may be protected as well down the line.

To conclude, as long as the Third-Party Doctrine is altered to allow people to have a reasonable expectation of privacy on sensitive data shared, the Fourth Amendment and the Third-Party Doctrine can co-exist for many years to come. It is possible that the Third-Party doctrine be discontinued, but it is unlikely to happen anytime soon.

# Where Does 21st-Century Data Fit in?

Today, we live in a society where companies love to toss our data around. Many mundane tasks require us to give away our data and information. Many companies abuse this, selling data that is unrelated to required business operations all to advertising companies. While most data is considered the same under the Third-Party Doctrine, many are pushing to get advertising data about users protected under the fourth amendment.

The issue dates to the explosion of the data collection economy with the introduction of the internet and smart phones. Companies can track people wherever they go. An employer can go to a company and look up data tied to a potential candidate, such as their internet searches. We are throwing away our privacy, yet, many people are unaware of how much about them is out there. Is privacy just an illusion?

In cases where the collection of data is obvious and practical, such as a phone company keeping a record of calls, Fourth Amendment protection should not apply. As long as the information is not sensitive to the user, the user would be less likely to expect privacy over it.

For companies which don’t use customer data to the user’s benefit, many agree the user deserves more protection. Greg Nojeim, who is a senior counsel at the Center for Democracy and Technology, and Orin Kerr, a George Washington University law professor, debated the issue. Nojeim argued, “If strict application of the doctrine ever served us well, it no longer does, leading to absurd results. This is particularly true in an age where so much more information is communicated through intermediaries” (John Villasenor, 2018, para. 9). Kerr added:

I think that the much-maligned third-party doctrine is a critical tool for applying the Fourth Amendment to new technologies in some cases, but that it should not be extended to all cases ... Importantly, my defense of the third-party doctrine implies an important limit: The doctrine should apply when the third party is a recipient of information, but it should not apply when the third party is merely a conduit for information intended for someone else. (John Villasenor, 2018, para. 9)

In summary, many agree that the doctrine should only apply for companies who use the data practically. Any information that companies hold on to just to sell would count under a reasonable expectation of privacy by the user, as the user wouldn’t expect their data to be used that way when signing for a service.

# Conclusion

To conclude, the Third-Party Doctrine once lived together peacefully with the Fourth Amendment, but the modern data age is calling for changes. The area which they conflict continues to grow as technology and law continue to develop. Over time, it is safe to expect seeing multiple cases concluding with refinements to the Third-Party Doctrine. The unanswered questions are: what will be protected next and will the Third-Party Doctrine eventually be obsolete?

The answer to what is a reasonable expectation of privacy will always vary person by person and case by case. However, there are also many things we agree on. Let’s continue to push for a future where data collection and protection are balanced perfectly to improve efficiency and quality of life while protecting people from unreasonable searches.

# References

Kemp, D. S. (n.d.). Smith v. Maryland, 442 U.S. 735 (1979). Retrieved from <https://supreme.justia.com/cases/federal/us/442/735/>

Lynch, J. (2017, September 20). Symposium: Will the Fourth Amendment Protect 21st-Century Data? The Court Confronts the Third-Party Doctrine. Retrieved September 26, 2018, from <http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/>

Olmstead v. United States. (n.d.). Oyez. Retrieved September 29, 2018, from <https://www.oyez.org/cases/1900-1940/277us438>

Ronald McLeod (2018). NSCC ISEC3050/Ethics and Law in Data Analytics, Halifax, Nova Scotia

Skelton, C. (n.d.). Katz v. United States, 389 U.S. 347 (1967). Retrieved from <https://supreme.justia.com/cases/federal/us/389/347/>

U.S. Constitution Annotated. (n.d.). Retrieved September 26, 2018, from <https://www.law.cornell.edu/constitution-conan/amendment-4/search-and-seizure>

Villasenor, J. (2013, December 30). What You Need to Know about the Third-Party Doctrine. Retrieved September 26, 2018, from <https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/>

Vogue, A. D., & Foran, C. (2018, June 22). Supreme Court: Warrant generally needed to track cell phone location data. Retrieved September 30, 2018, from <https://www-m.cnn.com/2018/06/22/politics/supreme-court-ruling-cell-phone/index.html?r=https://www.google.ca/>

Warren, S. D., & Brandeis, L. D. (1890, December 15). The Right to Privacy. Retrieved September 26, 2018, from <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>