**Online Writing Assignment 2**

**Expectations of Privacy in Cyberspace**

Adam Livingston

University of Arizona

CYBV 329 Cyber Ethics

Assistant Professor Heidi Calhoun-Lopez

26 June 2022

**Expectations of Privacy in Cyberspace**

**Introduction**

With the advent of cyberspace and the internet, along with revelations from Edward Snowden of bulk collection of metadata of all American citizens by the NSA, the concern of online privacy has catapulted to the forefront of legal and ethical discourse. Although seizure of traditional communications has long been debated since the invention of the telephone, the new frontier of cyberspace has added a new wrinkle in this discussion – how the Fourth Amendment applies to digital communications. **Privacy expectations in cyberspace apply to one’s communications that are not public, and seizure of said communications require a warrant. But willingness to publicly share communications (aka Third-Party Doctrine) do not have privacy expectations.** This paper will discuss in detail those privacy expectations, how to balance individual privacy with societal security, and how to apply the Fourth Amendment for emergent communication technologies.

**Comparing/Contrasting Physical and Digital Communications**

While in public and in publicly-accessible areas, there is not an expectation of privacy. This means that, according to Thompson II on *Katz v. United States* (1967) that the Fourth Amendment “left unprotected anything a person knowingly exposes to the public” (Summary). This is known as the “Third Party Doctrine”, meaning that once information is verbalized or published, it is no longer private and the recipient now has knowledge of or access to it. However, when someone “seeks to preserve as private, even in an area accessible to the public, [it] may be constitutionally protected” (6). This overturned the *Olmstead v. United States* (1928) case where the Supreme Court ruled that the Fourth Amendment does not apply to privacy in communications. Therefore, the Third Party Doctrine in the *Katz* case was established. So as the prevalence of telephone technology increased in the 39 years between *Olmstead* and *Katz*, the Supreme Court amended their thinking on Fourth Amendment applications. The interpretation of “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated” (Constitution) has now been extended to digital communications.

But what kind of digital communications are **not** protected? With the exponential growth of technology, we have seen the prolific rise of social media companies and users that post publicly-accessible information. Since these posts are able to be seen by the world, government agents do not need a warrant to view these communications. However, if someone posts them with viewing restricted only to their “friends”, and if a government agent is a friend of that individual, then those communications are not subjected to privacy expectations and once again, do not require a warrant. But if the post is private and unviewable by a government agent, then a warrant is necessary. However, according to the Third Party Doctrine, a non-government agent who is able to view those posts may report them to the proper authorities since those were “knowingly exposed to the public” since they now have knowledge of or access to it.

Taking the Third Party Doctrine and court precedent into account, we can define expectations of privacy with respect to digital communications and the Fourth Amendment. According to the Electronic Frontier Foundation’s article “Know Your Rights”, in order for a government agent/agency to seize your communications, a warrant is required. Additionally, a warrant is also required in order to extract content and other data off of digital devices. But, as with police wanting to enter a home without a warrant, “if [one gives] consent to a search, then the police don’t need a warrant… even if [one] is arrested” (2). Even if the police do have a warrant, it must be narrowly-tailored for that search (4-5).

With regards to emails, the Third Party doctrine is “[divided] along a content/non-content distinction” (Thompson II, 12). In simpler terms, the body of an email cannot be viewed without a warrant but the metadata (i.e., the header information and IP addresses, like the information on an envelope) can. This principle also applies to cell phone communications as determined in the *Carpenter v. U.S.* (2018) case. The case determined that cell phone location data requires a warrant because, if it didn’t, then the government could track all individuals that hold GPS-capable cell phones which “could…be extremely intrusive and damaging” (11). But like with metadata collection, the phone numbers dialed from a cell phone are covered by Third Party Doctrine (Thompson II, 12). Even so, courts have struggled to delineate the nuances of what data is considered private and subject to Fourth Amendment protections as there is a wide variety of data types with the emergence and ever-evolving cyberspace domain.

**Balancing Privacy and Security**

Balancing individual privacy with societal security is very subjective to individuals. On one extreme, some are willing to take a Hobbes-esque approach and forfeit all privacy in the name of security whereas others are unwilling to forfeit any privacy. There is a balance the lies somewhere in-between and is a matter of personal opinion. According to The University of Chicago Law Review, 52% of Americans are “concerned about government surveillance” and 65% “believe that there are inadequate limits on surveillance in place” (23). Even after the Snowden revelations, Americans are split on their concern about government surveillance even when informed about bulk-collection of their metadata.

Since this topic is subjective, the author of this paper is going editorialize his opinions regarding the balance of privacy and security. I believe that there is and should be no expectation of privacy in public, whether it be in traditional forums or publicly-posted social media content, so long as it meets the Plain View Doctrine. With the Snowden revelations and increasing mission-creep from police, privacy violations and warrantless searches by government agents is concerning and violates a fundamental right guaranteed to citizens. What makes this especially concerning is that the Supreme Court has ruled in *Frazier v. Cupp* (1969) that police and government agents may lie to suspects in order to elicit information regarding their investigation (Wikipedia). The only way for citizens to assert their rights in such an event is to know and articulate them in the face of substantial pressure during an interrogation. This is even more concerning since police, with the protection of qualified immunity, are “shield[ed]…from…liability when they perform their duties reasonably” (Cornell Law). But citizens, when ignorant of the law, are held to a standard that ignorance is not an excuse to be shielded from liability when breaking the law. Such is the problem if an officer lies with the threat of arrest in order to gain consent from a subject to search digital communications, or is just simply ignorant of their powers afforded to them as a government agent.

On the flipside, security is just as important as privacy but, to paraphrase Thomas Jefferson, rights should not be sacrificed in the pursuit of security. Surveillance on citizens should only be done when probable cause exists in order to obtain a warrant. In the *Katz* case, I believe that the Supreme Court was wrong in their decision that states metadata is not considered private as bulk-collection of that data that is then aggregated to paint a comprehensive picture of an individual can be extremely intrusive. However, foreign communications that are intercepted by intelligence agencies showing potential malice and harm towards the US and its citizens may be acted upon. FISA warrants are necessary for security but the main concern is abuse of the system as it was used to gain a warrant monitor the metadata of all Americans. Additionally, public communications may be acted upon to obtain further warrants as Third Party Doctrine applies with said communications.

In short, government agents/agencies have shown their willingness to abuse existing law and court precedent in order to further the pursuit of security regardless of harm it does to individual privacy. To balance the scales, there needs to be more of an emphasis placed on individual privacy with legal protections allotted to citizens that promotes accountability within the government. The balance lies within this accountability structure when ignorance of the law is no longer considered an excuse in the case of government agents and when they violate a citizen’s rights. Namely, removing qualified immunity protections will hold government agents to the same legal standard as citizens are expected to abide by. Arguably, removing the legal protection that police have to lie to suspects will help solidify the privacy rights of citizens as consent to search given under threat of arrest is an ethical gray area. Removing this protection may subject the officer to be accountable for their actions under 18 USC 242, Deprivation of Rights Under Color of Law (Department of Justice). But as long as probable cause exists, then warrants can be obtained for digital communications in order to pursue security.

**Emergent Technologies and the Fourth Amendment**

In *Olmstead v. US*, dissenting Justice Brandeis said, “experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding” (10). I agree with Justice Brandeis. The *Olmstead* case taught that emergent technology that was “without understanding” was abused by “well-meaning” government agents in the pursuit of justice. However, as determined in the *Katz* case, their decision was shown to be wrong as the technology gained widespread understanding.

Justice Brandeis’s sentiment can be expanded to future, unknown communications technologies. We do not know where the inventive human spirit will take our species in the realm of communications. But if we were to use history as a guide, we know that newer, faster, and more advanced methods of communication have yet to be developed. These technologies need to be subject to the Fourth Amendment protections which will future-proof citizens’ rights. As demonstrated above, government agents tend to abuse their authority in pursuit of justice which, in turn, bastardizes the very concept at the expense of citizens’ rights.

**Conclusion**

As illustrated above, privacy expectations in cyberspace apply to one’s communications that are not public, and seizure of said communications require a warrant. But willingness to publicly share communications do not have any expectation of privacy. The balance of privacy with security will be a subjective, ongoing debate that may shift the balance scales depending on major attacks on the homeland, such as it was after the September 11 attacks. Additionally, strong accountability structures need to put in place for government agents in order to protect citizens from negligent interpretation and corrupt abuses of the law. But one thing remains certain: Justice Brandeis’s dissent in the *Olmstead* case is a prophetic warning about how we treat emergent technologies with regards to Fourth Amendment and privacy protections. We should heed that warning and look at new communications technologies with a wary eye in how government approaches warranted and warrantless surveillance and seizures of individual communications.

**Works Cited**

“Can Americans Resist Surveillance?” *The University of Chicago Law Review*, vol. 83, no. 1, 2016, pp. 23–43. *JSTOR*.

Carpenter v. U.S. 585 US \_\_\_. Supreme Court of the US, 2018.

Constitution US. “Full Constitution of The United States - 2022.” *Constitution of the United States*, 26 May 2022, constitutionus.com.

“Deprivation Of Rights Under Color Of Law.” *The US Department of Justice*, 31 May 2021, www.justice.gov/crt/deprivation-rights-under-color-law.

“Know Your Rights.” *Electronic Frontier Foundation*, 2014, www.eff.org/issues/know-your-rights.

Olmstead v. U.S. 277 US 438. Supreme Court of the US, 1928.

“Qualified Immunity.” *LII / Legal Information Institute*, www.law.cornell.edu/wex/qualified\_immunity#:%7E:text=Qualified%20immunity%20is%20a%20type,duties%20reasonably.%E2%80%9D%20Pearson%20v. Accessed 21 June 2022.

Thompson II, Richard. “The Fourth Amendment Third-Party Doctrine.” Congressional Research Service, 2014, pp. 1–26.

Wikipedia contributors. “Frazier v. Cupp.” *Wikipedia*, 20 Apr. 2022, en.wikipedia.org/wiki/Frazier\_v.\_Cupp.