Princeton Legal Journal

Volume 2 Spring 2023

REVIEW

The Content-Specific Doctrine: The Right to be Secure in Digital Effects

Xander de los Reyes

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

— Amendment IV, US Constitution.

Introduction

The Fourth Amendment's original intent was to protect Americans from unreasonable searches and seizures.[1] At the time they were drafting the Constitution, the Founding Fathers remembered these violations of privacy as physical trespasses committed by British officials against colonists. This raises the question: Were the seizures of letters from a desk drawer or the broad searches of one's coat pockets unreasonable searches and seizures because they were physical in nature? Or were they violations of privacy because of the content searched and seized?

I argue that unreasonable searches and seizures can occur without physical intrusion. As technology becomes increasingly prevalent, violations of privacy can occur in non-physical realms (i.e., "cyberspace"). Although these violations lack the physical dimension that characterized early-American conceptions of Fourth

[1] U.S. Government Publishing Office, Constitution of the United States of America: Analysis and Interpretation, S. Doc. No. 112-112-9, 2d Sess. (June 27, 2016). https://www.govinfo.gov/content/pkg/GPO-CONAN-REV-2016/pdf/GPO-CONAN-REV-2016.pdf.

Amendment violations, they can nonetheless rise to a level of invasiveness that can be seen as functionally equivalent and can thus fall within the scope of the Fourth Amendment's prohibitions.

This piece proceeds in the following manner. First, I briefly outline the history of the Fourth Amendment and its original intent, which was to protect Americans' privacy from improper searches and seizures. Next, I outline twentieth-century case law that has shaped modern understandings of the Fourth Amendment. In this section, I also introduce the *third-party doctrine*, a legal doctrine that is troubling given society's contemporary dependence on technology. Then, I discuss technological consent—or the lack thereof. Finally, I introduce a new legal framework, the *content-specific doctrine*. Instead of focusing on the physical nature of a search or third parties involved, this doctrine considers the content of effects (personal belongings) seized to be the highest-order consideration. The content-specific doctrine can protect privacy, digital civil liberties, and Fourth Amendment rights in this technological age.

I. History

Under British rule, colonists were subject to documents known as *writs of assistance* or *general warrants*. Authorized by these documents, British authorities could enter colonists' homes without probable cause. They could search homes indiscriminately for prohibited items and seize them. Even worse for the colonists, these writs lasted throughout the ruling king's life and six months past their death.[2] These documents flagrantly subjected the colonists to unreasonable searches and seizures.

When King George II died in 1760, an opportunity to protest the warrants arose.[3] An advocate General from Boston, James Otis, rose to the occasion. Otis resigned his post and opposed the writs' renewal in court in February of 1761. He could have merely objected to renewal, but went further. He argued that the writs were incompatible with the English constitution and went on to say that the only valid writs were "special writs."[4] (These were analogous to today's specific and narrow search warrants.) Otis's argument in court was one of the first formal

[2] James M. Farrell, "The Writs of Assistance and Public Memory: John Adams and the Legacy of James Otis," *The New England Quarterly*79, no. 4 (2006): http://www.jstor.org/stable/20474493.
[3] Farrell, "The Writs."
[4] Farrell, "The Writs."

colonial challenges to British authority.[5] Scholars have also cited it as one of the earliest instances of colonial inclinations toward independence.[6]

Otis lost the case, but his passionate argument left impressions on attendees and those who later learned of the event. One of the audience members would recall Otis's speech fifty-six years later in a letter to a friend:

> *Every Man of an immense crowded Audience appeared to me to go away, as I did, ready to take Arms against Writs of Assistants. Then and there was the first scene of the first Act of opposition to the Arbitrary claims of Great Britain. Then and there the Child Independence was born.*[7]

These are the words of John Adams, America's first vice president and second president. For him, the colonial conception of privacy was not just something of value—it was the very thing that set the pursuit of independence in motion.

This incident demonstrates the tremendous extent to which the colonists and Founding Fathers valued privacy. The writers of the Constitution—as survivors of British rule and its indiscriminate supervision—knew the importance of individual privacy and sought to protect people against unreasonable searches and seizures.

Since the ratification of the Constitution, determining violations of the Fourth Amendment has been complicated. As the nation aged, new circumstances and considerations arose. The invention of new technologies like telephones and computers, in addition to the Americans' increasing dependency on business and service providers, has complicated Fourth Amendment jurisprudence. A synopsis of how courts have responded to these changes will prove useful.

II. Twentieth-Century Case Law

Unreasonable searches and seizures were inherently physical in nature during British colonial rule and the early generations of the United States. This remained the case until the late nineteenth century when the invention of the telephone allowed for non-physical violations of privacy.[8] Today, with the internet and

---

[5] Farrell, "The Writs."
[6] William B. Allen and Jonathan Gienapp, "Against Writs of Assistance (1761)," National Constitution Center, https://constitutioncenter.org/the-constitution/historic-document-library/detail/james-otis-against-writs-of-assistance-february-24-1761.
[7] John Adams to William Tudor, Sr., March 29, 1817, https://founders.archives.gov/documents/Adams/99-02-02-6735.
[8] "1870s – 1940s: Telephone," Elon University, https://www.elon.edu/u/imagining/time-capsule/150-years/back-1870-1940/.

interconnected world, physicality is not a requirement for a violation of privacy. This transition has created an entirely new subset of privacy rights: *digital civil liberties*. Next, I briefly outline case law of the twentieth century to show how courts responded to these technological changes.

A. *Olmstead v United States* (1928)[9]

During Prohibition, federal law enforcement was investigating Roy Olmstead, a suspected bootlegger. Agents installed wiretaps on his telephone without a warrant. The agents installed the wires in the basement of the building Olmstead resided in and dug up phone wires underneath the nearby sidewalk. Because no physical intrusions occurred against Olmstead, the government felt it did not need a warrant. Olmstead countered that the warrantless searches violated his Fourth and Fifth Amendment rights.

In a 5-4 decision, the Supreme Court ruled against Olmstead. Chief Justice William Howard Taft authored the majority opinion. In it, he stated that "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house" then no violation of the Fourth Amendment occurred. This ruling created a precedent that reemphasized the Fourth Amendment's focus on physical intrusions. For nearly four more decades, as technology developed and spread, this precedent would stand.

B. *Katz v United States* (1967)[10]

Federal law enforcement was investigating Charles Katz, a man suspected of illegal gambling. Knowing Katz used public phone booths, the government, acting without a warrant, utilized devices capable of eavesdropping and added them to the exterior of a phone booth. After they collected incriminating evidence, agents charged Katz with eight counts of illegal transmission of wagering information across state lines. After being convicted, he appealed his conviction and argued that the warrantless monitoring of his phone call violated the Fourth Amendment.

Reversing course from *Olmstead*, the Court ruled 7-1 in favor of Katz. Delivering the opinion of the Court, Justice Potter Stewart stated that the Fourth Amendment, "protects people, not places." The ruling also created the *reasonable expectation of privacy test*, which has two requirements:

---

[9] *Olmstead v. United States*, 277 US 438 (1928).
[10] *Katz v. United States*, 389 US 347 (1967).

1. The person whose Fourth Amendment rights have supposedly been violated must have had a subjective expectation of privacy.
2. That expectation must be one that society can recognize as reasonable.

An individual's Fourth Amendment rights are thought to have been violated if both conditions are affirmatively met. Failure to satisfy either condition would result in the determination that privacy rights were not violated.

The *Katz* ruling overturned the decision in *Olmstead.* It became the first landmark Supreme Court case that extended Fourth Amendment rights beyond physical intrusions, and its reasonable expectation of privacy test is still used today.

C. Third-Party Doctrine

Two cases in the 1970s, *United States v. Miller* and *Smith v. Maryland*, created a legal framework known as the *third-party doctrine.*[11] In both of these cases, the petitioners claimed that their Fourth Amendment rights were violated. The searches and seizures of each case lacked a physical component and involved a third-party, such as a phone company or bank. These circumstances forced the Court to confront when individuals' expectations of privacy were reasonable.

In *United States v. Miller*, the government accused Mitch Miller of not paying a liquor tax on distillation equipment. To investigate, federal law enforcement subpoenaed two of Miller's banks. Without a warrant, they obtained records of his accounts. These documents were subsequently used against Miller in court, where he was convicted. Miller appealed and argued that his Fourth Amendment rights were violated when his bank records were obtained without a warrant.

In *Smith v. Maryland*, Michael Lee Smith was believed to have robbed a woman. Law enforcement also suspected that he was continuously calling the victim to harass her about the robbery. To investigate, the government asked Smith's phone company to install a "pen register," or a device that captures numbers dialed but none of the content of a phone call. When records indicated that Smith dialed the victim's phone number, law enforcement was able to get a search warrant to find further evidence. Smith was later identified by the victim in a line-up and then convicted of robbery. He argued that the pen register violated his Fourth Amendment rights and appealed.

The Supreme Court ruled against the petitioners in both *Miller* and *Smith.* According to the Court, both men voluntarily gave their information to third parties

[11] *Miller v. United States*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979).

(Miller and his bank; Smith and his phone company). Doing so, in the Court's view, undermines the first requirement of the reasonable expectation of privacy test. When individuals provide information to third parties, they abandon any subjective expectation of privacy.

Taken together, the decisions in *Miller* and *Smith* created the third-party doctrine. Under it, the government's acquisition of information from third parties does not require a warrant. The soundness of this ruling was debatable in the 1970s. Today, however, society relies deeply on many more third-party services—many of them related to technology and the internet. Therefore, the third-party doctrine exposes Americans to significant intrusions of privacy.

III. Technology & Consent

With each passing day, technology becomes more interwoven into life. Many Americans use some form of instant messaging like iMessage, WhatsApp, or Facebook Messenger to communicate with family, friends, and coworkers. Some utilize navigation applications like Google Maps, Apple Maps, and Waze. When the COVID-19 pandemic began to shut down daily operations in 2020, workplaces, academic institutions, and other organizations moved to video-conferencing services like Zoom, Google Meet, and Microsoft Teams. All of these aforementioned services—whether they are used to video-call with grandparents or to navigate to a political rally—require the consent of users. Recalling the third-party doctrine, the proliferation of technology seems thorny at best and dire at worst.

A concerning fact is that most individuals do not attentively read the terms of service for these services. (User agreements such as "terms and services" go by other names: *terms and conditions*, *terms of use*, *end-user license agreement*, *service terms*, etc. While some lawyers may say there are slight variations between these definitions, they all functionally refer to a contract between a user and a provider of some service. Within this legal article, all of these terms are used synonymously.) Clicking or tapping the "I agree" box or button is, in the most literal sense, a check in the box for many people. This fact is tacitly, and sometimes explicitly, recognized by service providers. Amazon Web Services (AWS), for example, has included a clause referring to a zombie apocalypse in §42.20 of its service terms.[12] They state that a previously mentioned restriction shall not apply in the situation of:

[12] Amazon, "AWS Service Terms," Amazon Web Services, https://aws.amazon.com/service-terms/.

> *[A] widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization.*

AWS's inclusion of zombies in a legally-binding contract implies that many people do not read these terms. It is an "Easter egg" for some vigilant users—or scholars examining contractual consent and relationships—to find.

Other services have left even more ridiculous statements in their terms of service. *Purple*, a wireless network company in Manchester, UK, embedded a clause within their terms of service that bound those who agreed to 10,000 hours of community service. 22,000 people consented.[13] A European security firm, *F-Secure*, created a publicly available wireless hotspot for people and included in its terms of service that "the recipient agreed to assign their firstborn child to us for the duration of eternity."[14] *GameStation*, a UK video game retailer, included in their terms of service that users' agreement gave the company ownership of each user's "immortal soul."[15] In 2019, a high school teacher in Georgia won $10,000 when she read the terms of service for travel insurance from *Squaremouth*, which stated that the company would provide a reward to the first person who contacted the company in response to reading their terms of service.[16] These are half-comical, half-frightening examples of the lack of awareness that most users have about the contents of terms of service.

There are strong implications when the third-party doctrine, legally-binding terms of service, and users' failure to read those terms are considered together. Most users of a service are required to agree to terms of service—i.e., contracts—to use said service. Thus, they have consented to give information to a third party, thereby rendering that information subject to the third-party doctrine. With humanity's increasing dependence on technology and its abundance of terms of

---

[13] Alex Hern, "Thousands sign up to clean sewage because they didn't read the small print," *The Guardian*, July 14, 2017, https://www.theguardian.com/technology/2017/jul/14/wifi-terms-and-conditions-thousands-sign-up-clean-sewage-did-not-read-small-print.

[14] Tom Fox-Brewster, "Londoners give up eldest children in public Wi-Fi security horror show," *The Guardian*, September 29, 2014, https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause.

[15] Magazine Monitor, "A Case for Reading the Small Print," BBC, last modified November 18, 2013, https://www.bbc.com/news/blogs-magazine-monitor-24992518.

[16] Matthew S. Schwartz, "When Not Reading the Fine Print Can Cost Your Soul," *National Public Radio*, March 18, 2019, https://www.npr.org/2019/03/08/701417140/when-not-reading-the-fine-print-can-cost-your-soul.

service, there must be a new legal framework for determining privacy rights and digital civil liberties.

IV. The Content-Specific Doctrine

A doctrine that best protects Americans' privacy is one that I call the *content-specific doctrine*. This framework emphasizes consideration of the content being searched and seized by the government. How information is obtained—be it physically or digitally—and a third party's role are both considerations secondary to the content of a search. The doctrine's primary concern is the qualitative features of the effects to be searched—the pages in a journal, the audio of a phone call, or the metadata of one's social media account.

A. Content as Primary Focus

First, an example may elucidate why content is more important than physical circumstances or whether information was given to a third party. Consider the example of a "peeping Tom." John is sexually interested in his coworker, Jane. Motivated by voyeurism, he hopes to obtain nude photos of Jane by standing outside her residence and covertly taking photos. Because modern cell phones are capable of capturing high-quality images—some of which are now capable of 100x zoom—John knows that he can easily capture these photos from outside Jane's curtilage; he need not physically intrude.[17]

Although no physical trespass may occur, this act is clearly immoral. The reason rests solely on the content of the information acquired: Jane, in her home, nude, and with an incredibly reasonable expectation of privacy. Normative judgments are independent of whether the trespass was physical in nature. Although this example does not involve the government, it is a clear example of why the content of what is obtained is more important than the physical circumstances of the acquisition.

B. Doctrine Use

Consider an example of law enforcement using the third-party doctrine to surveil an individual suspected of aiding women in getting abortions in a state where

[17] "We need to talk about the Samsung Galaxy S22 Ultra's zoom photography." *TechRadar*. February 17, 2022. https://www.techradar.com/news/we-need-to-talk-about-samsung-galaxy-s22- ultra-zoom

they have been banned or heavily restricted.[18] Sarah, a resident of Texas, has publicly posted on social media that she wholeheartedly believes in bodily autonomy and would offer to drive women in need of an abortion to a provider. County sheriff's deputies suspect Sarah of following through on her statements and driving low-income women in Houston to and from illegal abortion providers. They are able to see through Texas Department of Transportation records that she drives a Toyota Camry. Deputies find out that Toyota's end user license agreement and privacy notice inform users that the company's "ConnectedServices" collects data on vehicle owners, including location and voice recordings.[19] Whether or not Sarah knows what she gave the car manufacturer permission to collect, deputies obtain records of her location and any voice recordings without a warrant.

In ascertaining whether Sarah's Fourth Amendment rights were violated, the content-specific doctrine first considers the qualitative nature of the effects obtained by police—driving location data and audio recordings. This information can be incredibly personal to an individual. In daily life, most people assume that their whereabouts are not being tracked by others. Similarly, the conversations had in cars are assumed to be private in nature. The primary focus of the doctrine considers these features. In this instance, both categories of information are intimate and personal.

To help understand the content searched and seized, physically analogous scenarios can be helpful. Without technology, deputies would need to do at least one of two things to track Sarah's whereabouts to the extent that Toyota's data is functionally capable of doing: affix a GPS device to her vehicle or physically follow her whereabouts. Likewise, to record the conversations inside her vehicle, law enforcement would need to install a microphone inside the cabin of her Camry. In the absence of a warrant, these actions violate the Fourth Amendment.

Bringing these two ideas together yields an answer. The contents of the effects that deputies seek to obtain from Toyota—location and audio—are deeply

---

[18] Given how recent the overturn of *Roe v. Wade* 410 US 113 (1973) is, whether abortion-restricting states will explicitly ban aiding and abetting abortions is a matter of debate. However, because states generally make aiding and abetting other crimes illegal, it is not unreasonable to think such policies will exist, be they de jure or de facto.

[19] "Privacy and protection," *Toyota*, April 11, 2022. https://www.toyota.com/privacyvts; "Toyota Vehicle End User License Agreement." *Toyota*. https://www.toyota.com/privacyvts/assets/images/doc/Vehicle%20Software%20End%20User%20License%20Agreement%20Toyota.pdfUlanoff, Lance.

personal. In physical circumstances, the search would be unreasonable without a warrant. Because the doctrine considers content as its primary focus, an answer is revealed: the government's warrantless acquisition of Sarah's location and voice recordings violated her Fourth Amendment rights.

The content-specific doctrine would not, however, protect the searches of Sarah's public social media posts. The content, publicly available speech, is not as personal of information as location or audio recordings. Just as Sarah cannot reasonably expect that the words she utters in a grocery store aisle are private, she cannot expect posts on public social media to be free from government observation.

C. *Carpenter v. United States* (2018)[20]

An excellent example of actual legal thinking akin to the content-specific doctrine is the majority ruling in *Carpenter v. United States*. Suspecting Timothy Carpenter of robbery, the government obtained information from Carpenter's cell phone service provider. Federal agents obtained "cell site location information" (CSLI) data that spanned 127 days. Over this duration, they collected 2,898 location points on Carpenter. This is an average of 101 data points per day. It can also be thought of as, on average, having one's location documented and retroactively collected every 14 minutes and 15 seconds from August 20 until Christmas. The matter of the case focused on whether the acquisition of CSLI, without a warrant, violated Carpenter's Fourth Amendment rights.

Fortunately for digital civil liberties, the Court ruled in favor of Carpenter. The majority opinion, authored by Chief Justice John Roberts, focused on the character of CSLI data and its investigative potential for law enforcement. The Chief Justice noted: "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." He further states that cell phone tracking is even more invasive than GPS-tracking a vehicle because individuals often leave their vehicles but most keep their cell phones on them at all times.[2] He emphasizes this habitual proximity by noting that 12% of surveyed Americans confess to using their phones in the shower. The Chief Justice also notes that previous attempts by the government to recreate suspects' past physical movements were limited by the sheer quantity of records and its ability to collect them. With CSLI, however, the government can achieve near-perfect surveillance. The Chief

[20] *Carpenter v. United States*, 585 US __ (2018).

Justice states that: "Only the few without cell phones could escape this tireless and absolute surveillance."

In ruling in Carpenter's favor, the majority opinion functionally used the content-specific doctrine. Rather than determining the warrantless acquisition of Carpenter's CSLI to be legal based on the third-party doctrine, the majority examined the content of the government's search and seizure. The content, Carpenter's whereabouts over a period of 127 days, was extremely sensitive information. The Court recognized this sensitivity and duly considered it to fall under the protections of the Fourth Amendment. In *Carpenter*, legal thinking similar to the content-specific doctrine recognized that the essence of information collected by the government was more important than the manner in which it was obtained.

It should be noted that the Court's ruling in *Carpenter* was split: it was a 5-4 decision. Authoring the dissent, Justice Anthony Kennedy argued that CSLI data is no different than other business records that a third party maintains, and as such, the third-party doctrine should apply in Carpenter. This dissent was joined by Justices Alito and Thomas. The latter Justice filed an additional dissent that emphasized focusing on the physical nature of searches. In it, Justice Thomas discusses other Fourth Amendment precedents. He references a pre-*Katz* case where a "spike mike" (a microphone that can be physically driven through walls and other barriers for the purpose of eavesdropping) was inserted by federal agents into an individual's home, without a warrant, which was clearly a physical violation of privacy.[21] Justice Thomas makes this reference to support his disagreement with the Court's decreased emphasis on physical circumstances since *Katz*.

Both dissents are grounded in reasoning that the content-specific doctrine would address. It would focus on the content obtained by the government. In this case, nearly 13,000 pieces of location information spanning a period longer than four months and documenting an individual's physical movements. The content-specific doctrine would acknowledge the intimacy of this information and recognize that its warrantless seizure functionally creates an Orwellian surveillance state. Regardless of whether Carpenter consented to give this information to a third party (Justice Kennedy's dissent) or the physical circumstances of the search and seizure (Justice Thomas's dissent), the content-specific doctrine would find such government actions to violate the Fourth Amendment.

[21] *Silverman v. United States*, 365 U. S. 505 (1961).

Opponents of the content-specific doctrine may say that it weakens the government's ability to investigate crime. I acknowledge the government's need to do so in order to maintain order. However, order can be maintained, and crime investigated, through legally granted search warrants. The Fourth Amendment states that, although people are free from unreasonable searches and seizures, they are not absolutely free from *reasonable* searches and seizures. Presumably, what constitutes a reasonable search is described in the amendment: those conducted with a warrant based on probable cause that "particularly [describes] the place to be searched, and the persons or things to be seized." This wording was an attempt to prevent broad searches like those conducted under general warrants and writs of assistance.

In the digital age, such a warrant could coexist with the content-specific doctrine. Investigators' efforts to obtain very specific information—say, a suspect's whereabouts in a two-hour window on a specific date—could be seen as narrow enough to constitute a reasonable search and seizure. Of course, some privacy rights advocates may disagree (and I myself have hesitations). However, I acknowledge that the law must always seek to prioritize individual liberties while also conceding that *some* circumstances exist where those liberties can be narrowly encroached upon. Therefore, the content-specific doctrine is not at odds with the government's acquisition of narrow and specific search warrants. Rather, it seeks to prevent, minimize, and rectify broad and warrantless searches in cyberspace—in other terms: unreasonable digital searches and seizures.

Conclusion

This article began with a question about the Founding Fathers' conceptions of privacy: "Were the seizures of letters from a desk drawer or the broad searches of one's coat pockets unreasonable searches and seizures because they were physical in nature? Or were they violations of privacy because of the content searched and seized?" After examining the Founding Fathers' proclivities for privacy, it should be clear the transgressive character of unreasonable searches and seizures rested not on their physicality but on the government's capture of private belongings and information. Privacy, for colonists and the Founding Fathers, was revered.

Knowing that non-physical violations of privacy exist, this article then considered twentieth-century Fourth Amendment case law, the third-party doctrine, and the implications of new technology. Taken together, they showed exploitative potential. In response, I provided a new legal framework for Fourth Amendment rights in cyberspace: the content-specific doctrine. Above physical circumstances

or the role of third parties, the doctrine considers the content of information obtained by the government.

This doctrine will not magically settle all debates on privacy. It does, however, provide jurists with a way to consider Fourth Amendment rights in cyberspace. As technology becomes unavoidably interwoven into society, the content-specific doctrine can help protect Americans' digital civil liberties. The people have a right to be secure in their digital effects.