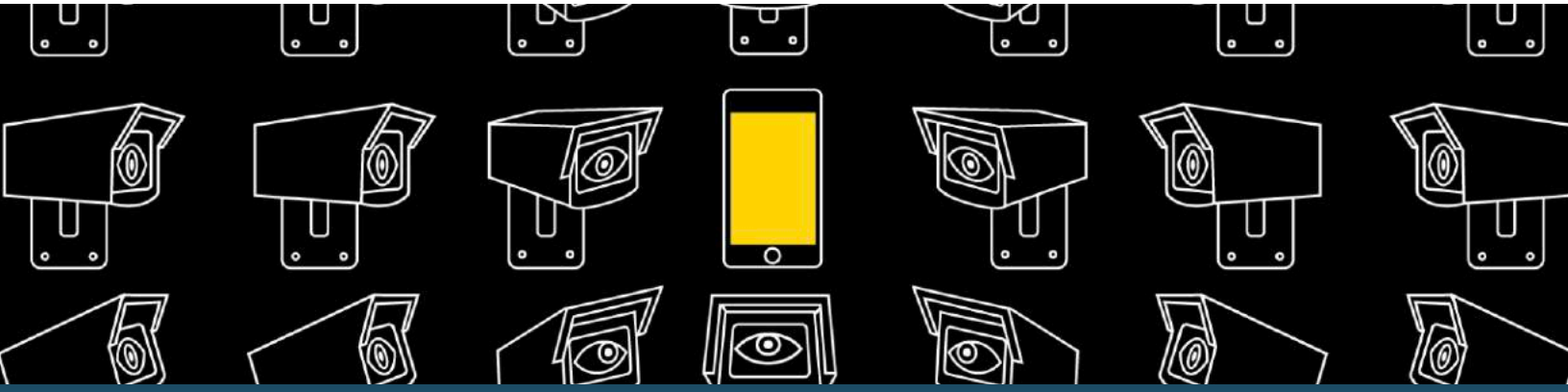
PUBLIC POLICY BRIEF

Protecting Your Digital Data from Warrantless Searches

LIBERTAS INSTITUTE



SUMMARY

"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."

These are the words that comprise the Fourth Amendment of the U.S. Constitution. Many defendants have relied on them—and similar clauses in state constitutions—but has modern technology rendered this protection ineffective? Has the traditional regard for privacy eroded to a point of no return? Can a 400-year-old idea continue to be relevant today?

The fears and concerns of the Constitution's drafters are as pertinent as ever today. New circumstances and technologies present themselves often, but there must be balance between the law and individual rights to ensure that our digital data is protected.

Our privacy interest in digital data stored with or created by a third party must be protected from warrantless searches.

This policy brief will outline the history of the U.S. Constitution's Fourth Amendment, specifically the provision regarding "the right of the people to be secure in their persons, houses, papers, and effects." The brief will explore how changes in technology have influenced the interpretation of this constitutional protection and will propose multiple avenues that can be pursued in order to ensure that this protection continues to be guaranteed for all Utahns and their digital data.

Fourth Amendment History

The basic framework of the Fourth Amendment was inspired by English Common Law. In 1604, the Semayne's case established the need for a warrant when searching someone's residence. The case involved a landlord attempting to collect property from an indebted, deceased tenant, but the deceased man's roommate would not allow entry. Sir Edward Coke, Attorney General of England at the time, said, "The house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose."[1]

Another case, *Entick v. Carrington*, established in 1765 the precedent that warrants were to be used when investigating private property and that they must be justified by probable cause. Using a general warrant from a government official, four men broke into the home of a writer (John Entick) who had been critical of the government in several newspapers. Entick promptly took them to court, and the chief justice ruled in his favor, finding the general warrant to have been unlawfully written. "[O]ur law holds the property of every man so sacred," wrote Lord Camden, the chief justice in the case, "that no man can set his foot upon his neighbour's close without his leave."[2]

The *Entick* case also distinguished between general and specific warrants, the latter of which deals with a particular person or place, narrowing law enforcement's focus to suspected criminal conduct. A general warrant, on the other hand, provides broad authority to search people and places not individually suspected of violating the law.

It is important to note that these types of protections did not carry over to the American colonies. In fact, until 1750, general warrants were the *only* kinds of warrants used. This produced what scholar William Cuddihy has termed the "colonial epidemic of general searches."[3]

One of the culprits in this general warrant epidemic were writs of assistance, which provided legal cover for officers (or anyone possessing the writ) to search homes, businesses, and other property at will, without having to articulate any suspicion of specific misconduct. As the British set about enforcing merchant laws and regulations, customs officials began to lean on these writs of assistance in order to conduct broad searches.

The irritation caused by these writs came to a head when King George II died in 1760. Writs of assistance expired six months after the death of the reigning monarch. A large number of Boston merchants took this as an opportunity to challenge the legality of the writs. They were represented by James Otis, whose fiery challenge of the authority of parliament left quite an impression on a young John Adams.[4]

Though James Otis lost the case, the event became one of many flashpoints leading to the American Revolution. In response to British enforcement of more draconian measures in 1767, most colonial courts began to refuse to issue general writs of assistance.

Prior to the drafting of the United States Constitution, several states drafted declarations of rights that included prohibitions of general warrants and searches. The Virginia Declaration of Rights from 1776 read, "General warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted."[5]

James Otis argues before the Superior Court of Massachusetts

The Massachusetts Declaration of Rights from 1780 likewise established a protection from "all unreasonable searches" that would later be used by James Madison when drafting the Fourth Amendment.[6]

In response to alleged deficiencies with the original Constitution, and echoing what several states had already asserted, James Madison drafted many amendments, including what became the Fourth Amendment. Madison's original draft included "other property," a more comprehensive term that would have potentially proved beneficial in our modern digital era. By March 1, 1792, it was adopted and ratified by the states and became a part of what is known now as the Bill of Rights.

Evolution of the Fourth Amendment

Federal courts dealt very little with the Fourth Amendment in the century following the Constitution's ratification since the federal government had hardly any jurisdiction in criminal law. As the federal government began to expand its reach to questions of interstate commerce, antitrust, narcotics, and organized crime, the U.S. Supreme Court began to interpret and clarify the application of this constitutional clause.

One of the first major cases was *Ex Parte Jackson* (1878), where law enforcement had been opening mail hoping to find illegal lottery materials. The Court ruled that letters and packages sent through the postal service were protected under the Fourth Amendment, establishing privacy in correspondence—an early indication that property enjoys privacy protections even when in the custody of a third party. In *Boyd v. United States* (1886) the Court unanimously held that the Fourth Amendment applied broadly to "all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life."[7]

Subsequent court rulings would begin to erode these protections, as was the case with *Olmstead v. United States* (1928) which, in a divided 5-4 vote, upheld the legality of government wiretapping of phone lines outside of a person's home without a warrant. Justice Louis Brandeis gave a notable dissent:

> *"Moreover, 'in the application of a constitution, our contemplation cannot be only of what has been, but of what may be.' The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. 'That places the liberty of every man in the hands of every petty officer' was said by James Otis of much lesser intrusions than these. To Lord Camden, a far slighter intrusion seemed 'subversive of all the comforts of society.' Can it be that the Constitution affords no protection against such invasions of individual security?"*[8]

The Fourth Amendment was born of a recognition of the need to protect privacy against unreasonable government intrusion.

Olmstead was eventually overturned in *Katz v. United States* (1967). This case dealt with the wiretapping of a public pay phone booth. Justice Marshall Harlan II wrote an important concurring opinion that defined a test for a person's reasonable expectation of privacy. "First that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[9] Charles Katz, having shut the phone booth door behind him, qualified under this standard for the expectation of privacy.

This test would eventually be adopted in *Smith v. Maryland* (1979) by the majority of the Court. Congress then codified the *Katz* case (and a similar one, *Berger v. New York* [1967]), in the Omnibus Crime Control and Safe Streets Act of 1968 to ensure that wired forms of communication (telephone, telegram, etc.) were covered by Fourth Amendment protections. The Electronic Communications Privacy Act of 1986 established the same for electronic communications. Similar attempts have been made recently via the Email Privacy Act to extend protections to emails held on a third party server, but they have not been so far successful in extending privacy of correspondence to this form of communication.

Prior to the passage of the Fourteenth Amendment and the development of the doctrine of incorporation, the

Bill of Rights (including the Fourth Amendment) did not apply to the states themselves, but only the federal government. This changed with *Mapp v. Ohio* (1961); the U.S. Constitution's privacy protections were extended to lower jurisdictions and are therefore applicable to state and local governments in Utah.

The Third Party Doctrine

An important facet of the Fourth Amendment is what has come to be known as the Third Party Doctrine. The question is: if a person voluntarily gives property, information, correspondence, etc., to a third party for storage or transport, does that person have a reasonable expectation of privacy?

Courts have struggled to adequately protect our privacy interest in data that is held by a third party.

California Bankers Assn. v. Shultz (1974) was an important initial case dealing with a law requiring banks to keep photocopies of the checks and transactions of their customers in case the government might want to review the records at some future date in an investigation. The U.S. Supreme Court upheld the law on a 6-3 vote, establishing that check owners had no reasonable expectation of privacy in the photocopied checks, but Justice Thurgood Marshall penned an interesting dissent:

> *"By compelling an otherwise unwilling bank to photocopy the checks of its customers, the Government has as much of a hand in seizing those checks as if it had forced a private person to break into the customer's home or office and photocopy the checks there. Our Fourth Amendment jurisprudence should not be so wooden as to ignore the fact that, through microfilming and other techniques of this electronic age, illegal searches and seizures can take place without the brute force characteristic of the general warrants which raised the ire of the Founding Fathers."*[10]

A similar case, *United States v. Miller* (1976), expanded the findings in *California Bankers Assn.* to include the use of subpoena powers against private third party bank information without obtaining a warrant. Again, Justice Marshall and Justice William Brennan dissented, arguing that bank customers have a reasonable expectation that the bank will keep their dealings confidential even as they voluntarily provide information to the bank.

Smith v. Maryland (1979) further expanded the Third Party Doctrine. In a 6-3 vote, a majority of the Court held that it was not a violation of the Fourth Amendment for law enforcement to access, without a warrant, a pen register—the log book of an individual's phone calls, kept by the phone company. Justice Marshall again dissented, arguing that a person had a reasonable expectation to privacy when making phone calls and that there are many legitimate reasons (unpopular political organizations, journalists with confidential sources, etc.) why someone would want to keep the details about those calls private.

Justice Potter Stewart's dissent also directly opposed the new standards of the Third Party Doctrine:

> *"The central question in this case is whether a person who makes telephone calls from his home is entitled to make a similar assumption about the numbers he dials. What the telephone company does or might do with those numbers is no more relevant to this inquiry than it would be in a case involving the conversation itself. It is simply not enough to say, after Katz, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police."*[11]

The Third Party Doctrine, established as a result of these cases, remains in force to this day in regards to federal interpretation of the Fourth Amendment. With the Internet's explosion in recent decades—and the increasing shift of human activity and content creation to the digital realm—this important debate has been reignited.

Technology and the Fourth Amendment

As we've entered the 21st century, the U.S. Supreme Court has taken a piecemeal approach to applying Fourth Amendment protections to new technologies. In one example, *Kyllo v. United States* (2001), the Court required law enforcement

officers to obtain a warrant before using thermal imaging devices on a person's home.

In another case, *United States v. Jones* (2012), the Court ruled against the use of a long-term GPS device for surveillance without a warrant. Justice Sonia Sotomayor gave an important concurring opinion:

> *More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.*[12]

The digital contents of a cell phone were protected from warrantless searches via *Riley v. California* (2014). In *Carpenter v. United States* (2018), the Court deviated from past case law to extend privacy protections to cell phone location information held by a third party.

Lower court rulings have also set the stage for ongoing reform on this topic. For example, the 6th Circuit Court of Appeals ruled on *Warshak v. United States* in 2010, holding that email communications are protected from warrantless searches. More specifically, the ruling prohibits the government from compelling an Internet Service Provider to provide those records without a warrant. Justice Danny Boggs wrote: "The Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[13]

This particular ruling is what motivated Congress to consider the Email Privacy Act, but at this point it has only passed the U.S. House of Representatives. Absent legislative reform, there is potential that the U.S. Supreme Court may, in a future case, apply these privacy protections to email communications.

Utah and the Fourth Amendment

When Utah became a state in 1896, the exact phrasing found in the Fourth Amendment was included in the Utah Constitution.

As technology has changed, the Utah Legislature has modified state law to enact privacy protections. In 1979 the Interception of Communications Act was passed to protect wire and oral communications from warrantless searches. In 1989 this was expanded to include electronic communications and where they are stored.

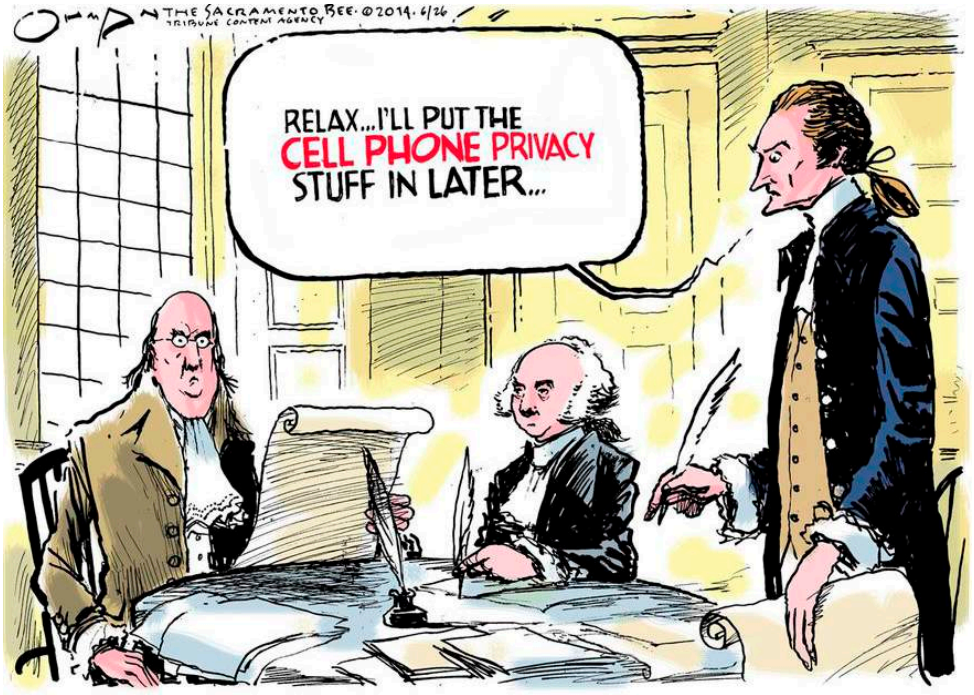
The Utah Legislature wasn't the only body willing to extend Fourth Amendment protections beyond U.S. Supreme Court precedent. The Utah Supreme Court weighed in on a case dealing with the privacy of bank records, similar to *United States v. Miller* in 1991. *State v. Thompson* reached a different conclusion to *Miller*, establishing protections for banking records, as several other states had done previously.[14]

More recently, House Bill 118, sponsored by Representative Daw and Senator Urquhart, was passed in 2012 to eliminate the exemptions that had been written into previous law that allowed warrantless searches of stored electronic data. Representative Wilcox and Senator Madsen sponsored House Bill 128 in 2014 which restricted the ability of law enforcement to obtain the content of electronic data transmissions from cell phones without a warrant. The bill was in response to new "stingray" technology that had been developed, allowing for bulk collection of cell phone data using mobile cell towers.

During the 2018 interim session, the Utah Legislature's combined judiciary committee held a hearing on the Third Party Doctrine and how privacy protections are affected by modern technology and people's perceptions of privacy. A proposal to legally protect third party data was recommended unanimously.

The Expectation of Privacy

Prior to the *Katz* ruling in 1967, Fourth Amendment protections were generally only tied to private property, particularly a person's home and letter correspondence. Even then, people had a general expectation that these items would remain private. As



society moved into the 21st century and people began to generate and disseminate vast amounts of private information electronically—via third party providers and especially using digital devices—there are new questions about people's expectations of privacy with the storage and transmission of this data.

It seems clear that the *contents* of digital devices and the phone calls made using those digital devices are protected by the Fourth Amendment. Even as late as 2018, location data from cell phones was recognized by the U.S. Supreme Court as subject to warrant requirements. But because of the Third Party Doctrine, the question remains: what about information stored on cloud storage or sent through third-party services?

People now store tremendous amounts of information in the cloud, whether it be photos and videos, financial records, business documents, or other sensitive and personal data. Third parties in the digital era facilitate this in two ways: they either provide storage for information, or they temporarily transmit information to and from separate digital devices as part of their service.

Parallels to these situations can be found in the physical world. First, you can entrust your property to a third party to store an item for a temporary period of time. By doing this, you do not forfeit your Fourth Amendment protections from a warrantless search for that item, even though it is no longer in your possession.

Second, when renting an apartment or staying at a hotel, you do not forfeit your privacy protections simply because a landlord, handyman, or maid has routine access to your room and belongings.[15]

In the same sense, when storing digital information with a third party or routinely allowing access to it by a third party service, you should not be compelled to waive your Fourth Amendment rights. This is the error of the logic of the current Third Party Doctrine. Electronic devices and third-party digital storage devices are repositories of our personal effects and should therefore be protected like their physical counterparts under traditional warrant requirements.

The Constitution is the Floor

Many people incorrectly believe that the U.S. Constitution and its interpretations from the U.S. Supreme Court are the final word on these types of issues. However, the Fourth Amendment was never meant to be treated as a ceiling. Congress and state legislatures across the country, for example, have been passing laws that extend greater protections of privacy rights for over two centuries.

Instead, the Constitution and Supreme Court rulings are rightly considered the floor—the minimum standard of protection for rights. While many states might be content with relying on this floor as the default standard, doing so misses an opportunity and perpetuates injustice.

The Utah Legislature Needs to Act

In *Riley v. California* (2014), Justice Alito wrote in his concurring opinion:

> *"It would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."*[16]

Utah need not wait for the U.S. Supreme Court to rule on every technological development, nor do we need to even agree with the level of protections the Court has afforded. The place to secure greater protections against warrantless searches of our data and information is through the state legislature.

PROPOSAL A: AMEND THE CONSTITUTION

We propose amending Utah's Constitution to explicitly ensure protection of digital data, as follows:

Article I, Section 14. [Unreasonable searches forbidden -- Issuance of warrant.]

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

PROPOSAL B: AMEND STATE LAW

Alternatively, similar protections can be enacted by changing statute as follows:

1. An individual who transmits electronic information or data to a remote computing service is presumed to be the owner of the electronic information or data.
2. The individual in Subsection (1) maintains a reasonable expectation of privacy in the electronic information or data stored by the remote computing service.
3. (a) Pursuant to Subsection 77-23c-102(1), a government entity may not obtain, use, copy, or disclose a person's electronic information or data stored by a remote computing service, or data the remote computing service generates in the course of the person's use of the service, without first obtaining a warrant.

   (b) Notwithstanding Subsection (3)(a), a government entity may obtain, use, copy, or disclose a person's electronic information or data stored by a remote computing service without a warrant:

   (i) with the informed, affirmative consent of the owner of the electronic information or data; or

   (ii) in accordance with judicially recognized exceptions to warrant requirements.

Endnotes

1. "Semayne's Case," Court of King's Bench, accessed January 14, 2019, https://groups.csail.mit.edu/mac/classes/6.805/admin/admin-fall-2005/weeks/semayne.html.
2. *Entick v. Carrington*, 19 Howell's State Trials 1029 (1765).
3. Leonard Williams Levy, *Seasoned Judgments: The American Constitution, Rights, and History* (Transaction Publishers, 1995), 150.
4. "James Otis' Fiery Rhetoric Sparked America's Revolutionary Fervor," Investors Business Daily, July 3, 2017, https://www.investors.com/news/management/leaders-and-success/james-otis-fiery-rhetoric-sparked-americas-revolutionary-fervor/.
5. "Virginia Declaration of Rights," http://avalon.law.yale.edu/18th_century/virginia.asp.
6. "Massachusetts Constitution," http://press-pubs.uchicago.edu/founders/documents/v1ch1s6.html.
7. *Boyd v. United States*, 116 U.S. 616 (1886).
8. *Olmstead v. United States*, 277 U.S. 438 (1928).
9. *Katz v. United States*, 389 U.S. 347 (1967).
10. *California Bankers Assn. v. Shultz*, 416 U.S. 21 (1974).
11. *Smith v. Maryland*, 442 U.S. 735 (1979).
12. *United States v. Jones*, 565 U.S. 400 (2012).
13. *USA v. Steven Warshak, et al*, No. 08-3997 (6th Cir. 2010).
14. *State v. Thompson*, 810 P.2d 415 (1991).
15. *United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997), *United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009).
16. *Riley v. California*, 573 U.S. ___ (2014).

PUBLIC POLICY BRIEF

Protecting Your Digital Data from Warrantless Searches

LIBERTAS INSTITUTE

FREQUENT RECURRENCE TO FUNDAMENTAL PRINCIPLES IS ESSENTIAL TO THE SECURITY OF INDIVIDUAL RIGHTS

UTAH CONSTITUTION
ARTICLE I, SEC 27

785 East 200 South, Suite 2, Lehi, UT 84043 | 801.901.0310 | LibertasUtah.org