



5-3-2025

YOUR DATA, MODERN TIMES, AND THE FOURTH AMENDMENT: WHAT WOULD JEFFERSON AND ORWELL DO?

Sterling, Ken

Follow this and additional works at: <https://digitalcommons.law.scu.edu/chtlj>



Part of the [Intellectual Property Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Sterling, Ken, *YOUR DATA, MODERN TIMES, AND THE FOURTH AMENDMENT: WHAT WOULD JEFFERSON AND ORWELL DO?*, 41 SANTA CLARA HIGH TECH. L.J. 47 (2025).

Available at: <https://digitalcommons.law.scu.edu/chtlj/vol41/iss1/2>

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized editor of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.

YOUR DATA, MODERN TIMES, AND THE FOURTH AMENDMENT: WHAT WOULD JEFFERSON AND ORWELL DO?

*Ken Sterling**

*The ongoing challenge of balancing individual data privacy with the government's need for user data through national security efforts has long plagued courts and policymakers. This tension intensifies as technology advances, permeating daily life, and global uncertainty fuels government demand for additional data. This study explores this tension by examining the Fourth Amendment's protection against unreasonable searches and seizures in the context of user data obtained by the government through third-party providers. I argue that the Fourth Amendment provides a sufficient framework to balance these competing interests. While acknowledging the government's responsibility for national security, we contend that this does not automatically override individual privacy concerns. However, the legality of the government purchasing third-party user data – data voluntarily provided by users to private companies – remains a critical question. Drawing on relevant case law, including *United States v. Jones*, this study analyzes the evolving legal landscape regarding user data and government surveillance. I conclude by calling for further discussion on the legality of government access to third-party data and exploring potential solutions within the existing framework.*

* Ken Sterling is a graduate of the USC Gould School of Law and an attorney in Media and Privacy Law in Century City, California. He was selected to SuperLawyers – Rising Stars in 2025 and he is an Associate Professor at the USC Gould School of Law. His research interests are at the intersection of media, law, and technology.

CONTENTS

| | | |
|------|--|----|
| I. | INTRODUCTION | 49 |
| A. | <i>Can the Government Purchase Third-Party Data and Get Around the Warrant Requirement Required by Carpenter v. United States?</i> | 50 |
| II. | FOURTH AMENDMENT, COURT CASES, AND FEDERAL PRIVACY LAWS | 53 |
| A. | <i>The Fourth Amendment</i> | 53 |
| B. | <i>Reasonable Expectation of Data Privacy: How Does the Fourth Amendment Apply?</i> | 56 |
| C. | <i>What is Surveillance, and When is a Warrant Required?</i> | 58 |
| D. | <i>Other Court Cases and Regulations that Relate to Data Privacy</i> | 61 |
| III. | ANALYSIS AND MODERN-DAY APPLICATION OF DATA PRIVACY LAW | 64 |
| IV. | CONCLUSION AND FUTURE CONSIDERATIONS FOR PROTECTING PRIVACY IN THE DIGITAL AGE | 66 |

I. INTRODUCTION

What if the attacks on September 11, 2001, had been prevented? What about the school shootings that plague our nation today? Government agencies claim that when they access larger quantities of user data from United States (U.S.) citizens, they can better prevent or detect crime.¹ Individuals, civil liberty organizations, and legal experts are in an uproar about “Big Brother,” and clamoring for a change in the Fourth Amendment, seeking more restrictions on the government and its use of private user data.² This raises questions about individual data privacy rights and balances them against the government’s claim that a greater amount of data is needed to keep the nation and people safe. The government claims that these data are needed to thwart criminals and evildoers in the interests of national security. However, the irony, *and* bitter truth is that private user data *has been voluntarily given away by them* in exchange for access to free applications such as Google Search, Gmail, Facebook, Instagram, YouTube, and TikTok. Why should the Courts place a higher standard on the government’s use of commercially available user data? Recently, the government has purchased data from third-party data providers such as Fog Data Science, LLC.³

Although it is hard to fathom that Jefferson, Madison, and our forefathers had any idea the Internet, social media or other technology would exist, it still is possible to rely on the basic foundation of the Fourth Amendment, when it comes to balancing an individual's right to privacy with the interests of the government to protect the American people. On one hand, the government claims the need for national security, thwarting terrorism, and stopping crimes is of paramount priority. For them, this means aggressive and liberal interpretations of the Fourth Amendment to allow access to more data, which results in less privacy for U.S. Citizens, foreign nationals, and corporations. On the other hand, civil rights proponents claim the government has become “Big Brother” and is violating the rights of private citizens

¹ See U.S. Gov't Accountability Off., *Protecting Personal Privacy*, <https://www.gao.gov/protecting-personal-privacy> (last visited Feb. 13, 2025).

² See *NSA Spying*, ELEC. FRONTIER FOUND., <https://www.eff.org/nsa-spying> (last visited Feb. 13, 2025).

³ Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget*, ASSOCIATED PRESS (Sept. 1, 2022), <https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef> (it was founded in 2016 by two former U.S. Department Homeland Security employees).

with Section 702,⁴ FISA,⁵ and PRISM.⁶ While these two sides argue the merits of their positions, experts wonder: *How can we follow laws that were enacted nearly 250 years ago, when Jefferson and Madison had no idea what was coming?*

The answer to the Fourth Amendment conundrum lies in a more nuanced view. Courts can apply the legislative intent of the Fourth Amendment to all data privacy questions so that the government should be able to utilize third-party data that users supplied voluntarily, requiring no revisions regarding the Fourth Amendment of the U.S. Constitution.

A. *Can the Government Purchase Third-Party Data and Get Around the Warrant Requirement Required by Carpenter v. United States?*

Regarding the Fourth Amendment and the government's use of third-party data without a warrant, the Courts' answers range from *maybe* to *yes*.⁷ This is because users have given third-party companies consent to store and share data as business records, and the companies have authority over such records.⁸ Common Authority allows the third-party company to consent to a government search of its data, even if the user opposes it.⁹ Furthermore, third-party companies may enter into voluntary sales ("manifested consent") of user records that would otherwise be protected by the Court's decision in *Carpenter v. United States*.¹⁰

A recent example of such data exchange is the arrangement between Fog Data, LLC, and the U.S. government. There has been much controversy surrounding the government's use of this data, and some believe that the government is using this information to conduct

⁴ Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified in scattered sections of 50 U.S.C.).

⁵ Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

⁶ PRISM government data surveillance software enabled by Protect America Act of 2007 and FISA. Glen Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, THE GUARDIAN (June 6, 2013), <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

⁷ See Oren Kerr, *Buying Data and the Fourth Amendment*, HOOVER INST. AEGIS SERIES PAPER NO. 2109 (2021).

⁸ *Id.* at 3.

⁹ *Id.* at 1.

¹⁰ *Carpenter v. United States*, 138 S. Ct. 2206, 2209 (2018).

illegal surveillance of its citizens.¹¹ At the heart of this controversy is Fog Data's purchase and aggregation of sensitive user information from tech companies, followed by the sale of this data to the government.¹² Critics claim that Fog Data's and the government's use of user data violates constitutional individual privacy rights; the government should not have access to this information because it undermines civil liberties and establishes dangerous precedents for future information sharing.¹³ Others contend that the government must have access to these data to prevent and respond to national security threats.¹⁴ It is crucial for ensuring public safety.

Concerns also exist regarding the need for greater transparency surrounding how the government uses this data.¹⁵ Many feel that there must be greater oversight or accountability regarding data management, as discussed further by the Brennan Center for Justice.¹⁶ How the information is being used and who has access to it requires clarification. In addition, concerns exist about Fog Data's security, as hackers have allegedly breached systems and stolen sensitive data.

Overall, the debate over the government's use of Fog Data is likely to remain unresolved for some time. Although strong arguments exist on both sides, this issue raises important questions regarding privacy, security, and civil liberties. As technology and safety requirements evolve, new challenges regarding data privacy will emerge. Advances in computer technology have led to the development of new surveillance tools to collect large amounts of data from a wide range of individuals. More third-party data collection companies, like Fog Data, sell data to the government, likely bypassing the need for search warrants or probable cause.

Apple's stance on government access to user data has fluctuated. While previously cooperating in cases involving child exploitation, the company forcefully resisted an FBI demand to unlock a terrorist's iPhone. CEO Tim Cook argued that compliance would

¹¹ See Matthew Guariglia, *What is Fog Data Science? Why is the Surveillance Company so Dangerous?*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), <https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous>.

¹² *Id.*

¹³ *Id.*

¹⁴ See *Protecting Personal Privacy*, *supra* note 1.

¹⁵ See Rachel Levinson-Waldman et al., *Social Media Surveillance by the U.S. Government*, BRENNAN CTR. FOR JUST. (Jan. 7, 2022), <https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government>.

¹⁶ *Id.*

undermine civil liberties. To further bolster user privacy and deter future government requests, Apple has implemented robust encryption for user data and devices, potentially exacerbating tensions with law enforcement. In some prior law enforcement situations, Apple had been open to sharing information with the government to thwart crimes against children,¹⁷ except when Apple refused to share this data with the government for surveillance purposes.¹⁸ Signaling a significant swing away from government cooperation, Apple refused to unlock a device belonging to a suspected terrorist who killed fourteen people and injured twenty-two others.¹⁹ Published in an open letter and posted on Apple's website,²⁰ Apple CEO Tim Cook stated, "We feel we must speak up in the face of what we see as an overreach by the U.S. government." Cook further explained that, "We are challenging the FBI's demands with the deepest respect for American democracy and a love of our country. Ultimately, we fear that this demand would undermine the very freedoms and liberties our government is meant to protect."²¹ Apple's desire to appeal to additional users who want to feel their data is private, and to block further government requests for user data, resulted in Apple recently announcing a revision of user data encryption in the Apple Cloud system, "beef[ing] up user security, [which is] risking law enforcement ire."²² Apple has now stated that it

¹⁷ Jack Nicas, *Apple's iPhones Will Include New Tools to Flag Child Sexual Abuse*, N.Y. TIMES (Aug. 5, 2021), <https://www.nytimes.com/2021/08/05/technology/apple-iphones-privacy.html>.

¹⁸ Kif Leswing, *Apple Will Reject Demands to use CSAM System for Surveillance*, CNBC (Aug. 9, 2021), <https://www.cnbc.com/2021/08/09/apple-will-reject-demands-to-use-csam-system-for-surveillance-.html>.

¹⁹ Katie Benner et al., *Apple's New Challenge: Learning How the U.S. Cracked Its iPhone*, N.Y. TIMES (Mar. 29, 2016), <https://www.nytimes.com/2016/03/30/technology/apples-new-challenge-learning-how-the-us-cracked-its-iphone.html>; see Katie Benner and Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), <https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html>; see also Eric Lichtblau, *In Apple Debate on Digital Privacy and the iPhone, Questions Still Remain*, N.Y. TIMES (Mar. 28, 2016), <https://www.nytimes.com/2016/03/29/us/politics/in-apple-debate-on-digital-privacy-and-the-iphone-questions-still-remain.html>.

²⁰ Tim Cook, *A Message to our Customers*, APPLE (Feb. 16, 2016), <https://www.apple.com/customer-letter/>.

²¹ *Id.*

²² Robert McMillan et al., *Apple Plans New Encryption System to Ward off Hackers and Protect iCloud Data*, WALL ST. J. (Dec. 9, 2022),

will encrypt user data and devices, making it impossible to view or share the data.²³

In other recent developments, bipartisan efforts have resulted in the drafting of legislation that would prohibit the government from purchasing personal data (such as that from Fog Data, LLC).

In 2021, a Bill was introduced by twenty-one prominent U.S. Senators,²⁴ including Ron Wyden (Democrat) and Rand Paul (Republican), to stop “shady data brokers from buying and selling Americans’ constitutional rights.”²⁵ In their introduction to the “Fourth Amendment is not for Sale Act,” Senator Mike Lee stated, “The federal government should not be allowed to skirt the Fourth Amendment’s existing warrant requirements and surveillance laws by purchasing Americans’ data from third-party brokers. This legislation will protect Americans’ civil liberties by closing loopholes in the existing law.”²⁶ More than a year later, despite the bill’s impressive sponsorship, it did not progress.²⁷ This is likely because most lawmakers agree with this study’s thesis: we do not need new or expanded laws for data privacy, as they relate to the government’s use of third-party data that users have voluntarily relinquished. The next section analyzes the Fourth Amendment as it pertains to data privacy laws.

II. FOURTH AMENDMENT, COURT CASES, AND FEDERAL PRIVACY LAWS

A. *The Fourth Amendment*

In its entirety, the Fourth Amendment states:

<https://www.wsj.com/articles/apple-plans-new-encryption-system-to-ward-off-hackers-and-protect-icloud-data-11670435635>.

²³ Arielle Waldman, *Experts applaud expansion of Apple’s E2E encryption*, TECHTARGET (Jan. 23, 2023), <https://www.techtargget.com/searchsecurity/news/252529487/Experts-applaud-expansion-of-Apples-E2E-encryption>.

²⁴ Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. (2021) (as introduced, Sen. Ron Wyden, Apr. 21, 2021).

²⁵ Ron Wynden, *Wynden, Paul, and Bipartisan Members of Congress Introduce the Fourth Amendment is not for Sale Act* (Apr. 21, 2021), <https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act->.

²⁶ *Id.*

²⁷ S. 1265, 117th Cong. (2021) (died in committee).

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.²⁸

To better understand the intent of the Fourth Amendment, it is helpful to imagine the smoke-filled rooms of the 1700s and the spirited debates about how to craft the Bill of Rights. After the reign of King George, our forefathers wanted to ensure that U.S. citizens would be protected against unreasonable searches and seizures by the government.²⁹ They were concerned about protecting themselves from tyranny like that of King George's army, which unlawfully broke into homes, offices, wagons, and ships.³⁰ Although Jefferson and Madison had no inklings about the Internet, social media, or cloud data, they did have an elegant notion of what privacy should be.³¹ On the one hand, there are the rights of individuals and their reasonable expectations of privacy, as well as their right not to have items, or data, seized without probable cause or a warrant. However, governments must keep the country and communities safe from terrorists, criminals, and other national security threats.

With recent technologies, including the Internet and a person's ability to be anywhere in the world and yet still "connected" to the U.S., this issue raises interesting questions. Businesses also qualify under the Fourth Amendment to the extent that they expect privacy and the right to be free of unlawful searches and seizures. However, as discussed here, under *Smith v. Maryland*,³² and *United States v. Miller*,³³ business records and individual records voluntarily shared with a third party are most likely not protected under the Fourth Amendment. This is also known as the Third-Party Doctrine, as further explained in *United*

²⁸ U.S.CONST. amend. IV.

²⁹ Laura Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1327 (2016).

³⁰ *Id.* at 1240-44.

³¹ See Daniel Solove, *A Brief History of Information Privacy Law*, 6 J.L. & POL'Y INFO. SOC'Y. 1, 3-5 (2006) (discussing early American privacy principles).

³² *Smith v. Maryland*, 442 U.S. 735 (1979).

³³ *United States v. Miller*, 425 U.S. 435 (1976).

States v. Miller,³⁴ which means there is no expectation of privacy in information voluntarily in business records provided to others, or third-parties.³⁵

In the 1700s, people had private homes, documents, and business records. Arguably, this still applies to modern society, user data, and business records, which are the same types of data that could have been stored and accessed using traditional methods, such as paper and file cabinets. Or should it? For example, is GPS data subject to search and is a warrant required to obtain it? The U.S. Supreme Court answered this question in 2012 in their ruling *United States v. Jones*,³⁶ deciding that an individual's GPS data was private and that the government needed to have a search warrant to collect and use such data.

The U.S. Supreme Court then made a landmark decision in *Riley v. California*³⁷ in 2014, ruling that the unwarranted search for and seizure of the digital contents of a cell phone during an arrest was unconstitutional under the Fourth Amendment. By contrast, the Third-Party Doctrine, established by *Smith v. Maryland*,³⁸ held that there is no reasonable expectation of individual privacy in records of dialed telephone numbers, which a telephone company stores in the ordinary course of business.

The courts will likely find that data sharing and selling agreements between the government and third-party providers (such as Fog Data³⁹) will not be subject to Fourth Amendment requirements or require a warrant.

Similarly, it is probable that courts will find that location data transmitted by a cell phone to a cell carrier, sold to third parties, and then repackaged in the aggregate for the government are not subject to a reasonable expectation of privacy (even if the cell phone user has no reason to expect the government to compel the service provider to disclose the data). In these cases, the courts will most likely apply the

³⁴ *Id.* at 443.

³⁵ Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH L. REV. 561, 566 (2009).

³⁶ *United States v. Jones*, 565 U.S. 400, 404 (2012).

³⁷ *Riley v. California*, 573 U.S. 373, 387 (2014).

³⁸ 442 U.S. at 738.

³⁹ Bennet Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), <https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police>.

rationale of the lower appellate court in *Riley*⁴⁰ or *Carpenter*,⁴¹ explaining that “where any member of the public could have observed the defendant's movements, it cannot possibly be a Fourth Amendment violation for the government to monitor those movements using cell phone locations.”⁴²

Generally, it is acceptable for a private (non-governmental) technology company to collect, use, and sell individual user data, provided that the user has consented to such data use. This consent is usually accomplished by the user accepting “cookies” on websites or accepting the terms of service (TOS) or the end user license agreement (EULA) in a software application. The question becomes: can the government purchase and utilize user data from a technology company if the user voluntarily provides the data? The most likely answer is yes, and *Fog Data*⁴³ is an example of this. In the recent case, *Sanchez vs. Los Angeles Department of Transportation*,⁴⁴ the court ruled that it was permissible to collect and use data from the Los Angeles Department of Transportation, a government actor, and the Third-Party Doctrine applies to the use of the data.⁴⁵

B. *Reasonable Expectation of Data Privacy: How Does the Fourth Amendment Apply?*

Currently, a fine line exists between what constitutes a reasonable expectation of privacy and when authorities may conduct a lawful search without probable cause or obtaining a warrant. Some legal experts argue that new legislation is needed to address these concerns because current laws and precedents are outdated and, consequently, inadequately protect individual rights.⁴⁶ However, as this thesis states, lawmakers and courts must only look at the Fourth Amendment’s legislative intent and apply modern-day common sense to new data privacy considerations. Otherwise, court systems and legislatures will be mired in a voluminous and overwhelmingly

⁴⁰ 573 U.S. at 373.

⁴¹ 138 S. Ct. at 2246.

⁴² *Riley*, 573 U.S. at 373.

⁴³ *Cyphers*, *supra* note 39.

⁴⁴ *Sanchez v. L.A. Dept. of Transp.*, 35 F.4th 548 (9th Cir. 2022).

⁴⁵ *Id.* at 562.

⁴⁶ See Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264 (2004).

codified system of laws, similar to Napoleonic Law, which is only applied in one state in the U.S.: Louisiana.⁴⁷

There have been several seminal court cases related to data privacy, each of which has significantly affected how courts view the importance of protecting personal data. One of the earliest cases was *Olmstead v. United States*⁴⁸ in 1928, in which two men were convicted of illegal wiretapping. In this case, the U.S. Supreme Court considered and ruled on whether wiretapping constitutes an illegal search under the U.S. Constitution.⁴⁹ Arguably, telephones and wiretapping are related to data privacy, and this was a precursor of other such cases to come. In *Olmstead*, the Court ruled that a warrant was unnecessary and that the Fourth Amendment had not been violated because there was no search for or seizure of the defendant.⁵⁰ At the time, the Court believed that wiretapping and recording conversations did not amount to searching for or causing seizures.⁵¹ Courts later altered their stance on this issue, as technology evolved and embraced these changes with new frameworks and balancing tests.

Two modern court cases have been pivotal in shaping the legal standards for individuals' reasonable privacy expectations. The first case is *Katz v. United States*, in which the Supreme Court established that the information we share with others, such as conversations in public places—or, in the future, our keystrokes on a computer—is not protected under the Fourth Amendment.⁵² The Supreme Court held that the Fourth Amendment protected people rather than places.⁵³ This case established the Reasonable Expectation of Privacy test,⁵⁴ which is still used today to determine whether a search or seizure is unconstitutional.⁵⁵

The second seminal case is *Kyllo v. United States*,⁵⁶ which held that the police may not use thermal imaging technology to scan a

⁴⁷ See A.N. YIANNPOULOS, LOUISIANA CIVIL LAW SYSTEM: COURSEBOOK 1–3 (1977) (explaining that Louisiana's legal system is derived from the Napoleonic Code and remains distinct from common law jurisdictions).

⁴⁸ *Olmstead v. United States*, 277 U.S. 438 (1928).

⁴⁹ *Id.* at 466.

⁵⁰ *Id.* at 462.

⁵¹ *Id.* at 466.

⁵² *Katz v. United States*, 389 U.S. 347, 360 (1967).

⁵³ *Id.* at 351.

⁵⁴ *Id.* at 361 (Harlan, J., concurring).

⁵⁵ See, e.g., *Carpenter*, 138 S. Ct. at 2213.

⁵⁶ *Kyllo v. United States*, 533 U.S. 27 (2001).

private home without obtaining a warrant.⁵⁷ While these cases have established legal standards for law enforcement officers to conduct lawful searches, many recent developments have expanded their power to conduct searches in new and increasingly invasive ways. For example, in some instances, the police can demand that individuals unlock their devices with biometric features, such as thumbprint readers and facial recognition software, without obtaining a warrant.⁵⁸ There has been a conflicting decision by a California judge which does not broadly allow the use of biometrics to unlock devices.⁵⁹ This will likely make its way up to the Supreme Court of the United States as this is an important issue. The recent use of warrantless searches in law enforcement is controversial because it creates dangerous tension between private rights and public safety, which can be resolved by updating the legislation. While some argue that judges already have the authority to limit searches, others believe that law enforcement agencies should be given greater leeway to maintain public safety as technology advances.

C. *What is Surveillance, and When is a Warrant Required?*

Government surveillance involves monitoring the activities of individuals and groups using government agencies. Modern-day surveillance includes monitoring GPS locations, internet usage, phone calls, text messages, social media posts, and other types of communication. Governments cite many reasons for believing it is necessary to engage in surveillance, including national security, stopping criminal activity, enforcing laws and regulations, and gathering information for intelligence purposes.⁶⁰ Several government agencies, including the Federal Bureau of Investigation (FBI), police departments, the Central Intelligence Agency (CIA), the National Security Agency (NSA), and other state government agencies, such as Departments of Motor Vehicles, regularly conduct government surveys and data gathering.⁶¹ The government also contracts with private companies that conduct surveillance activities or aggregate data and

⁵⁷ *Id.* at 37.

⁵⁸ *United States v. Payne*, No. 22-50262, slip op. at 12 (9th Cir. Apr. 17, 2024).

⁵⁹ *In re Search of a Residence in Oakland, California*, 354 F. Supp. 3d 1010 (N.D. Cal. 2019).

⁶⁰ *See Protecting Personal Privacy*, *supra* note 1.

⁶¹ *Id.*

sell them to the government, such as Fog Data.⁶² While some legal experts express concerns about the implications of surveillance by the government, others claim that it is vital that surveillance continues so that the government can protect the general public.

Governments use various surveillance techniques. One common method is the wiretapping of phone calls or Internet usage, which involves attaching listening devices to phone lines or monitoring Internet traffic in real time.⁶³ Another common surveillance and security method is the use of publicly visible cameras, particularly traffic cameras, or, in some cases, spy cameras, which allow government agencies to monitor people's activities without their knowledge.⁶⁴

Several seminal cases have considered surveillance and the need for warrants. One of the most important is *Smith v. Maryland*,⁶⁵ which established that there is no reasonable expectation of privacy for information voluntarily communicated to third parties such as phone companies. The Supreme Court held that the police could obtain telephone records without a warrant because people did not have a reasonable expectation of privacy in such records.⁶⁶ This ruling was subsequently expanded in *United States v. Miller*,⁶⁷ which determined that financial records held by third-party banks also did not fall under reasonable expectations of privacy.

As mentioned above, one of the most significant Supreme Court cases dealing with the Fourth Amendment and privacy rights was *US v. Jones* in 2012, which dealt with the government's use of a GPS-tracking device.⁶⁸ In this ruling, the Court held that installing a GPS device on a suspect's vehicle to track his or her movements constituted a search under the Fourth Amendment and therefore required a warrant.⁶⁹ The case involved the arrest of a drug dealer who was found to possess cocaine after being tracked for several weeks by law

⁶² Cyphers, *supra* note 39.

⁶³ Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523.

⁶⁴ U.S. Dep't of Justice, *Criminal Resource Manual* § 32, *Video Surveillance—Use of Closed-Circuit Television (CCTV)*, <https://www.justice.gov/archives/jm/criminal-resource-manual-32-video-surveillance-use-closed-circuit-television-cctv> (last visited Feb. 13, 2025).

⁶⁵ *Smith*, 442 U.S. at 743-744.

⁶⁶ *Id.*

⁶⁷ *Miller*, 425 U.S. at 442.

⁶⁸ *Jones*, 565 U.S. at 412.

⁶⁹ *Id.* at 413.

enforcement officials.⁷⁰ They had attached a GPS tracking device to the car the suspect was driving, allowing them to follow his movements and gather evidence against him.⁷¹ However, the defense argued that this constituted an unreasonable search and seizure in violation of the Fourth Amendment, as neither Jones nor his car was seized. In the unusual 9-0 ruling, the Supreme Court agreed with the defendant's argument and determined that warrants were required for GPS devices that track people on public property.⁷² However, given that GPS technology has become so common, it remains to be seen how this ruling will impact future cases and what other new technologies might also fall under the protection of the Fourth Amendment.

Other key cases in this area include *Riley v. California*, which held that the police needed a warrant to search for the contents of a cell phone seized from a person who had been arrested.⁷³ In *State of Iowa v. Sanders-Galvez*, the Supreme Court ruled that a subject's Internet search history could be used as evidence in criminal trials.⁷⁴ *Carpenter v. United States* further addresses the legality of collecting cell phone records and other digital communication data from private companies.⁷⁵ These cases continue to shape the legal framework of current and future government surveillance. They underscored the justification for not creating new laws or modifying the Constitution concerning data privacy.

Courts have recently shared their views on the modern-day definitions of reasonable expectations of privacy and protection against unreasonable searches and seizures. For example, they have provided guidance on questions such as the collection (seizure and search) of data.⁷⁶ Is this a fundamental right protected by the Fourth Amendment? The answer is, *it depends*, and this lies at the intersection of two different topics: the first is an individual's expectation of privacy. The second is what information, or data, a person keeps to themselves versus what they share with others. The topic of the government's ability to obtain user information from third-party providers introduces the Third-Party Doctrine, as previously discussed in the *Smith*⁷⁷ and

⁷⁰ *Id.* at 402.

⁷¹ *Id.* at 403.

⁷² *Id.* at 413.

⁷³ 573 U.S. at 401.

⁷⁴ *State v. Sanders-Galvez*, No. 17-2059 (Iowa Ct. App. May 15, 2019).

⁷⁵ 138 S. Ct. at 2217.

⁷⁶ *Riley*, 573 U.S. 373; *Sanders-Galvez*, No. 17-2059 (Iowa Ct. App. May 15, 2019); *Carpenter*, 138 S. Ct. 2206.

⁷⁷ 442 U.S. at 743-744.

*Miller*⁷⁸ cases. In both matters, the U.S. Supreme Court held that bank records were not subject to protection under the Fourth Amendment because they were voluntarily shared with a third party, the bank.⁷⁹ The Third-Party doctrine is true even if the individual assumes that a third party will use the data for a limited scope or purpose. This guidance from the courts also means that the government can generally obtain data from a third-party business records relating to the individual (suspect) without a warrant or violation of Fourth Amendment protections.⁸⁰

D. *Other Court Cases and Regulations that Relate to Data Privacy*

One of the more recent cases regarding the U.S. government and data privacy is *Carpenter v. United States*, which decided whether law enforcement agencies could obtain cell phone location data without a warrant.⁸¹ In this case, Timothy Carpenter was convicted of several armed robberies based on cell phone location evidence that the FBI obtained without a warrant.⁸² Carpenter argued that this violated his 4th Amendment right against unreasonable searches and seizures.⁸³ The Supreme Court ultimately ruled in the government's favor, finding that there was no reasonable expectation of privacy for cell phone location data; therefore, government agencies did not need to obtain a warrant before accessing it.⁸⁴

Another important case relating to the U.S. government and data privacy is *Smith v. Maryland*, which assessed government agencies' ability to obtain certain types of digital records without a warrant.⁸⁵ In this case, a robbery suspect was arrested after the police obtained his call log information through a pen register device attached to his phone line under an order that had not required the police to demonstrate a "probable cause."⁸⁶ The Supreme Court ruled in favor of law enforcement, finding that the Fourth Amendment did not protect information voluntarily shared with a third party, such as phone

⁷⁸ 425 U.S. at 435.

⁷⁹ *Smith*, 442 U.S. 735; *Miller*, 425 U.S. 435.

⁸⁰ *Smith*, 442 U.S. 735; *Miller*, 425 U.S. 435.

⁸¹ *Carpenter*, 585 U.S. at 300.

⁸² *Id.* at 302-3.

⁸³ *Id.*

⁸⁴ *Id.* at 320-21.

⁸⁵ *Smith*, 442 U.S. at 735.

⁸⁶ *Id.* at 737.

records.⁸⁷ This ruling has been widely criticized by privacy advocates and tech companies, who argue that it has allowed for the mass surveillance of digital communications without adequate oversight or warrants.⁸⁸

In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA), lowering the standard for the government to obtain a warrant for surveillance that relates to foreign intelligence gathering and concerns about US citizens suspected of espionage.⁸⁹ To obtain a FISA warrant, the FISA court (also created by the Act) must find probable cause indicating that the individual being targeted is an agent acting on behalf of a foreign power.⁹⁰

After the 09/11 terrorist attacks, the Bush Administration ordered the National Security Agency (NSA) to implement domestic wiretaps without warrants.⁹¹ The justification was preventing future terrorist attacks.⁹² Additionally, a program was created to collect the bulk data of anyone who could be a perceived threat to U.S. national security, including individuals who were American citizens.⁹³ This program, run by the NSA, is known as PRISM.⁹⁴ In 2013, Edward Snowden leaked information about PRISM to the public and the

⁸⁷ *Id.* at 743-44.

⁸⁸ Hanni Fakhoury, *Smith v. Maryland Turns 35 and Its Health Is Declining*, ELEC. FRONTIER FOUND. (June 3, 2014), <https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining>.

⁸⁹ Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1813.

⁹⁰ Foreign Intelligence Surveillance Act, 50 U.S.C. § 1805(a)(2).

⁹¹ Jameel Jaffer, *A Brewing Battle Over Warrantless Wiretapping*, ACLU (Feb. 15, 2012), <https://www.aclu.org/news/national-security/brewing-battle-over-warrantless-wiretapping>.

⁹² U.S. Dep’t of Just., *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006), <https://www.justice.gov/archive/opa/docs/whitepaperonnsalegalauthorities.pdf>.

⁹³ Privacy & Civ. Liberties Oversight Bd., *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court 1* (Jan. 23, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/cc542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf.

⁹⁴ *Id.*

program came under intense scrutiny, resulting in a backlash and new laws that reduced its and related programs' power.⁹⁵

In 2007, President Bush signed the Protect America Act of 2007 (PAA),⁹⁶ amending FISA⁹⁷ to loosen the warrant requirements for tapping phone calls originating in or being received from foreign countries. Several PAA provisions were reauthorized in the FISA Amendments Act of 2008⁹⁸ and have been cited as the legal basis for continuing the mass surveillance methods previously revealed by Snowden (which were then ordered to be halted).

In 2001, the U.S. Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act),⁹⁹ expanding both the ECPA¹⁰⁰ and FISA¹⁰¹, and granting more authority to federal law enforcement to combat terrorism through surveillance. In May 2011, President Obama signed the PATRIOT Sunsets Extension Act of 2011, which extended roving wiretaps and searches of business records.¹⁰² The extension expired in 2015 when Congress enacted the USA Freedom Act: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act, restoring several PATRIOT Act provisions.¹⁰³ The USA Freedom Act somewhat limited the surveillance powers of the FBI and NSA, although not to the degree that civil liberties advocates had advocated for.¹⁰⁴

⁹⁵ *Id.*

⁹⁶ George W. Bush, President of the U.S., *Remarks on the Protect America Act of 2007* (Sept. 19, 2007), in *National Security*, George W. Bush White House Archives, <https://georgewbush-whitehouse.archives.gov/infocus/nationalsecurity/text/>.

⁹⁷ FISA Amendments Act of 2008, H.R. 6304, 110th Cong. § 702 (2008).

⁹⁸ FISA Amendments Act of 2008, H.R. 6304, 110th Cong. (2008).

⁹⁹ PATRIOT ACT. Public Law 107-56 107th Congress. (2001).

¹⁰⁰ Electronic Communications Privacy Act of 1986 (ECPA). (1986).

¹⁰¹ FISA Amendments Act of 2008, H.R. 6304, 110th Cong. (2008).

¹⁰² PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216.

¹⁰³ USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268,

¹⁰⁴ Neema Singh Guliani, *What's Next for Surveillance Reform After the USA Freedom Act*, ACLU (June 3, 2015), <https://www.aclu.org/news/national-security/whats-next-surveillance-reform-after-usa-freedom-act>.

III. ANALYSIS AND MODERN-DAY APPLICATION OF DATA PRIVACY LAW

The evidence presented in the literature reviewed here demonstrates that the Fourth Amendment has been correctly applied in cases that involve data privacy, and that there is no need to create new laws to address technology advances. Based on the case law, the published opinions of the Justices, and even dissenting opinions, it is clear the courts have aptly been applying the Fourth Amendment, developing relevant frameworks and tests that create sound legal precedents to later be applied by lower courts.

The analysis can be relatively simple if we distill it into the following question: what if we could have prevented the attacks on 09/11? Based on the answer to that question, we can determine how to balance individual and government needs to stop terrorism while simultaneously protecting privacy. Undoubtedly, questions have been raised about the Fourth Amendment in seminal court cases such as *Carpenter v. U.S.*¹⁰⁵ and *Smith v. Maryland*.¹⁰⁶ With the recent developments in government purchasing data from third-party providers, such as Fog Data,¹⁰⁷ these debates continue. Indeed, nearly ten years ago, the revelations by Edward Snowden rocked the data privacy world and revealed that the government has been collecting substantial amounts of personal data without warrants for decades.¹⁰⁸

Turning on the news, reading a paper, or scrolling on social media makes clear that the debate regarding the government's supposed broad and unlawful breach of data privacy continues. In 2020, the FBI conducted as many as 3.4 million warrantless searches for electronic data.¹⁰⁹ The searches were made possible by section 702 of FISA, which allowed the government to collect communications

¹⁰⁵ 138 S. Ct. at 2217.

¹⁰⁶ 442 U.S. at 735.

¹⁰⁷ Cyphers, *supra* note 39.

¹⁰⁸ Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>; Mirren Gidda, *Edward Snowden and the NSA Files - Timeline*, THE GUARDIAN (Aug. 21, 2013), <https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>.

¹⁰⁹ Dustin Volz, *FBI Conducted Potentially Millions of Searches of Americans' Data Last Year, Report Says*, WALL ST. J. (Apr. 29, 2022), <https://www.wsj.com/articles/fbi-conducted-potentially-millions-of-searches-of-americans-data-last-year-report-says-11651253728>.

from U.S. companies without a warrant.¹¹⁰ The report issued in 2022 by the U.S. Justice Department's Office of the Inspector General sent shockwaves through the American public, regarding the number of warrantless searches conducted.¹¹¹

A subsequent report published in 2024 by the Director of National Intelligence revealed further increases in FISA searches¹¹² and inspired more ire from the public and legal experts. Further underscoring the controversy about FISA searches and a potential shift by Courts, a very recent groundbreaking decision by a federal court, in *United States v. Hasbajrami*,¹¹³ ruled that warrantless searches conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA) can violate the Fourth Amendment. This ruling marks the first time a court has found such searches unconstitutional, following years of public scrutiny over the government's use of Section 702 to conduct warrantless surveillance on Americans, including activists, members of Congress, and journalists.

Regardless of Fourth Amendment or even the recent ruling in *Hasbajrami*,¹¹⁴ how can someone who wears a Fitbit and HealthRing, or one who regularly posts on social media about their personal life, assert that they have any expectation of privacy concerning that (or similar) data? They voluntarily relinquish their privacy and then complain the government has access to their data. Clearly, it is time for the pundits and critics to pick a side and one that aligns their ideology with their practicality of daily life.

Based on the research and analysis in this article, the question posed in the introduction has been answered in the affirmative. "Is the Fourth Amendment for sale?"¹¹⁵ The answer is *yes*, based on the *Smith*¹¹⁶ and *Miller*¹¹⁷ cases, plus an analysis of the circumstances involved in new matters, with the need to balance national security needs. The next question is whether the government can access private

¹¹⁰ FISA Amendments Act, *supra* note 4, at § 702.

¹¹¹ Volz, *supra* note 109.

¹¹² Office of the Dir. of Nat'l Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year 2023* (Apr. 2024), https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

¹¹³ *United States v. Hasbajrami*, No. 11-cr-00623 (LDH) (E.D.N.Y. Jan. 21, 2025).

¹¹⁴ *Id.*

¹¹⁵ Wyden, *supra* note 25.

¹¹⁶ *Smith*, 442 U.S. 735.

¹¹⁷ *Miller*, 425 U.S. 435.

data from third-party providers without obtaining a warrant or probable cause. The analysis and ultimate response here is the same: *yes*. The government should be able to access third-party user data without a warrant, provided that such data was legally shared with the third party, and more specifically where the third-party doctrine would already be applicable.

IV. CONCLUSION AND FUTURE CONSIDERATIONS FOR PROTECTING PRIVACY IN THE DIGITAL AGE

The challenge of balancing the individual's need for data privacy against the government's need to access user data to protect the U.S. and its citizens has long plagued policymakers. This will continue as long as we exist as a species. I am not sure if Jefferson and Madison would have any better answers to these legal questions than the ones our courts are providing today. However, one thing is for sure; as world development continues, technology continues to proliferate in our everyday lives, and with additional terrorist attacks and global uncertainty, the government will continue its quest to obtain more data.

The literature review and analysis presented here demonstrate that we do not need to create new laws on data privacy despite rapid technological advances. Furthermore, this study supports the view that the government may purchase third-party data on individuals from private companies without obtaining a search warrant, provided that those users have consented to such use and to possibly sell their data through a data software application or website. While readers of George Orwell's *1984* might decry the intrusion of "Big Brother" in the lives of private citizens, the threat of terrorism demands a more nuanced position. At the heart of this issue is a fundamental clash between competing values. On the one hand, we must maintain privacy to protect individuals from surveillance or harassment by government officials; on the other hand, we must safeguard communities from threats such as terrorism and cybercrime, which often rely on access to personal information.