The Fourth Amendment Judicial Understanding: Third Parties

Sophia Reiss[5]

ABSTRACT: *This article explores the Fourth Amendment's privacy protections specifically focused on the "third party exception" and the integrity of that exception to the Fourth Amendment and its definitions of privacy. Additionally, this article examines the European Union's relatively new data privacy law as an alternative way to account for third parties while remaining faithful to the Fourth Amendment's privacy ideals.*

The Fourth Amendment grants rights to privacy and protection from unnecessary government intrusion. Justice Louis Brandeis' dissent in *Olmstead v. United States* deepened the understanding of what the Fourth Amendment protects, specifically what privacy means. This includes detailing what is allowed as a search and seizure under the specified definition of privacy. This understanding of the Fourth Amendment and its purpose serves as background to the "reasonable expectation of privacy" test that protects situations where there is a reasonable expectation of privacy. *Maryland v. Smith* contributed the "third party exception" to the judicial understanding of the Fourth Amendment. The "third party exception" is when the government is allowed to access information revealed to a third party without obtaining a warrant. This exception lessens the privacy protections against government intervention, and should therefore be abolished as it does not fit with Justice Brandeis' explanation of the Fourth Amendment given technology's new role in our lives. Nowadays, it is hard to live a modern life without giving information to third parties as third parties have become so intertwined in our lives especially in the case of technology for example a smartphone is akin to a tracking device.[6] Despite technology and a lack of privacy pervading, "Americans say they care deeply about protecting their data" according to the Pew Research Center.[7] Unlike the United States government, the European Union has worked to take account of this disparity. The European Union wrote a data privacy law in 2016 in recognition of this new relationship with technology and the reasonable expectation of privacy that individuals expect in their interactions with technology.

The Fourth Amendment's meaning has evolved since its creation with *Olmstead v. United States (1928)* becoming a crucial precedent. Justice Brandeis thought that the wire-tapping of Olmstead violated the Fourth Amendment because the government violated Olmstead's privacy. Justice Brandeis wrote that the founders wrote the Fourth Amendment "to protect Americans in their beliefs, their thoughts, their emotions, and their sensations" and against "unjustifiable

[5] Undergraduate at Brandeis University Class of 2023.

[6] Manoush Zomorodi, "Do You Know How Much Private Information You Give Away Every Day?," *TIME*, March 29, 2017, https://time.com/4673602/terms-service-privacy-security/.

[7] Zomorodi, "Do You Know How Much Private Information You Give Away Every Day?"

intrusion by the government upon the privacy of the individual."[8] As Brandeis elaborates that "the privacy of the individual" includes "their beliefs, their thoughts, their emotions, and their sensations."[9] Brandeis explained that privacy considerations would have to evolve over time and that given the potential of possible new innovations the founders allow for the Fourth Amendment protections to expand.

The "third party exception" contradicts the reasonable expectation of privacy test because it does not fit with Brandeis' rationale for the Fourth Amendment. In *Maryland v. Smith*, the Supreme Court included the "third party exception" into the legal framework of the Fourth Amendment. The majority opinion explained that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[10] Returning to Brandeis' explanation, individuals are protected "in their beliefs, their thoughts, their emotions, and their sensations."[11] Even when expressing these protections to a third party, there is an expectation of privacy. For instance, when people have secrets they are often shared with a third party, but still treated as private information. The individual with the secret may "voluntarily" divulge the information to a friend, but this thought can still be regarded as private. This contradiction invalidates the "third party exception" to the legal understanding of the Fourth Amendment's privacy protections.

In *United States v. Jones* (2012), the U.S. Supreme Court decided the ways in which information may be obtained by the government without a warrant. The court stated that gathering copious amounts of a wide range of information without a warrant might violate the Fourth Amendment's right to privacy. In *Jones*, the court mentioned that "[i]t may be that achieving the same result [as traditional surveillance] through electronic means, (..) is an unconstitutional invasion of privacy," but Justice Scalia writing for the court chose to limit his discussion of electronic surveillance, focusing instead on the physical violation of the "search" provision of the Fourth Amendment.[12] In contrast to *Maryland v. Smith*, *Jones* outlines the core of the Fourth Amendment protections, which are grounded in intrusion on privacy of ideas often thought of as private property. Additionally, *United States v. Jones* portrayed how tracking methods can retain copious amounts of information of an individual's whereabouts violates the Fourth Amendment. *Jones* decided whether information obtained by installing a GPS on someone's car can be used as evidence against them. As Justice Sotomayor wrote in her *Jones*

[8] "Olmstead v. United States, 277 U.S. 438 (1928)," Justia Law, accessed November 23, 2019, https://supreme.justia.com/cases/federal/us/277/438/.
[9] "Olmstead v. United States, 277 U.S. 438 (1928)."
[10] "Smith v. Maryland, 442 U.S. 735 (1979)," Justia Law, accessed November 23, 2019, https://supreme.justia.com/cases/federal/us/442/735/.
[11] "Olmstead v. United States, 277 U.S. 438 (1928)."
[12] "UNITED STATES v. JONES," LII / Legal Information Institute, accessed November 23, 2019, https://www.law.cornell.edu/supremecourt/text/10-1259.

concurrence, “GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”[13] This statement demonstrates that tracking someone’s whereabouts gathers information that is beyond what would be obtained by other methods not involving a warrant. The “third party exception” counters this statement because when “a wealth of detail” similar to this is given to the third party the “third party exception” would decide that this information is no longer private.[14]

Technology has proven to be pervasive in society blurring the boundaries of privacy which should lead to a reexamination of the “third party exception.” Similarly to the GPS tracking in *Jones*, browser histories gather a plethora of information regarding personal matters which individuals would have a reasonable expectation of privacy. The “third party expectation” would not protect the privacy of browsing histories, private accounts, and websites. In the case of browser histories, internet providers, third parties, have access to the information of what one searched and everything one did online. Browsing histories are similar to the “papers and effects" that are protected by the Fourth Amendment and individuals would have a reasonable expectation of privacy in this information.[15] According to a Harvard Law Review article, “[v]iewing collection[s] of data" should be viewed as a Fourth Amendment search as people reasonably expect this data, and other online data, to be private.[16] This may fall within Justice Brandeis’ explanation that the Fourth Amendment “protect[s] Americans in their beliefs, their thoughts, their emotions, and their sensations.”[17] Browsing histories contain information often over long periods of time and with a range of kinds of information: business and personal.

Similar to browsing histories, private social media accounts contain a copious amount of information which might be understood by individuals to be private. On various social media platforms, individuals may create private accounts where they have control over what people can see, and who can access their account. The information may be posts, messages, or other potentially personal information which should similarly fall within the “papers and effects” protected by the Fourth Amendment. Additionally, private accounts would be reasonably understood to carry with a reasonable expectation of privacy given their namesake as “private” accounts. Since the social media platforms have access to information in all accounts, the individuals would have given away this information to a third party losing all rights to its privacy

[13] “UNITED STATES v. JONES.”
[14] “UNITED STATES v. JONES.”
[15] U.S. const. amend. 4
[16] “DIGITAL DUPLICATIONS AND THE FOURTH AMENDMENT,” *Harvard Law Review* 129, no. 4 (2016): 1046–67.
[17] “Olmstead v. United States, 277 U.S. 438 (1928).”

under the "third party exception" idea. This reality conflicts with their reasonable expectation of its privacy.

The "third party exception" should be abolished because technology grants third parties access to information which individuals still believe is private. Legal professions have noticed that technology's changing role in society will affect privacy protections. As Justice Alito stated in his *Jones* concurrence, "hypothetical reasonable person has a well-developed and stable set of privacy expectations" and "[b]ut technology can change those expectations."[18] The European Union acknowledged this new relationship between technology and privacy with its data privacy law.

The European Union privacy law regulates what third parties can do with the information given to them, which has created a culture where European individuals expect a high level of privacy regarding information and their technology. To make individuals aware of technology companies' interactions with their data and to provide individuals with greater control of their data, privacy law "would force Internet companies like Amazon.com and Facebook to obtain explicit consent from consumers about use of their personal data, delete that data forever at the consumer's request and face fines for failing to comply."[19] These companies' form of obtaining consent is generally through terms and conditions. While some may argue that terms and conditions are valid forms of obtaining consent, terms and conditions tend to be written to encourage compliance and they often are hard to read, long, and complicated. Many do not read through the terms and conditions and as "researchers estimate [it] would take 76 hours a year to read all the user agreements we meant" while "clicking 'No' often means not using a tool that you may actually need to navigate, communicate or work."[20] The European Union data privacy law takes into account this understanding of how we interact with these user agreements. Part of the privacy law's implementation includes requiring user agreements to be short, clear, and understandable. Through "obtaining explicit consent from consumers" this law insures the individuals' awareness that they are giving their information to a third party.[21] Given the ability of the consumers to "delete that data forever" with a request, they have additional control potentially expanding the boundaries of privacy protections within law especially with regard to data that third parties had access to.[22] The European data privacy law is more faithful to the Fourth Amendment's protection of privacy in the face of new technology.

---

[18] "UNITED STATES v. JONES."
[19] Somini Sengupta, "Europe Weighs a Tough Law on Online Privacy and User Data," *The New York Times*, January 23, 2012, sec. Technology, https://www.nytimes.com/2012/01/24/technology/europe-weighs-a-tough-law-on-online-privacy-and-user-data.html.
[20] Zomorodi, "Do You Know How Much Private Information You Give Away Every Day?"
[21] Sengupta, "Europe Weighs a Tough Law on Online Privacy and User Data."
[22] Sengupta, "Europe Weighs a Tough Law on Online Privacy and User Data."

Additionally, the expectation of privacy could change with greater awareness derived from companies' presentation of privacy agreements. Satariano states that "[a] central element of Europe's new regulations is that companies must clearly explain how data is collected and used."[23] This element could appear in a variety of ways, but would potentially produce a greater awareness of technologies' role in our lives and refine individual's expectations of what information is private.[24] The "third party exception" would most likely be resolved by these new regulations which could possibly appear in the United States. The potential of privacy legislation is shown through the European Union serves as an example for the United States as the author states "Europe's experience is being closely watched by policymakers in the United States, who are considering a new federal privacy law."[25] While legislation would change the manner in which the "third party exception" is discussed, the possibility of it in the future shows an acknowledgment of technological changes and crucial interactions with our privacy.

Due to the changed relationship between third parties and private information, the "third party exception" should be abolished. The "third party exception" introduced in *Maryland v. Smith* starkly contrasts with the understanding of the Fourth Amendment established in Brandeis' memorable *Olmstead* dissent. This dissent has framed discussions of the Fourth Amendment within the court's judicial opinions. In *Jones*, the justices debated the extent to which technological surveillance could be used under the Fourth Amendment. Providing further backing to abolish the "third party exception" is the European Union's new data privacy law which gives a crucial current acknowledgment of the changing nature of privacy. The "third party exception" would allow for information considered private within a reasonable expectation of privacy to be searched like browser histories and private accounts. Americans would benefit from a greater sense of privacy and security backed by real control over their information. It also could increase public trust in government and a real understanding of the benefits of governmental intervention.

[23] Adam Satariano, "Google Is Fined $57 Million Under Europe's Data Privacy Law," *The New York Times*, January 21, 2019, sec. Technology, https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.
[24] Satariano, "Google Is Fined $57 Million Under Europe's Data Privacy Law."
[25] Satariano, "Google Is Fined $57 Million Under Europe's Data Privacy Law."

Works Cited

Satariano, Adam. "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog." *The New York Times*, May 24, 2018, sec. Technology. https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

———. "Google Is Fined $57 Million Under Europe's Data Privacy Law - The New York Times," May 24, 2018. https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

Sengupta, Somini. "Europe Weighs Tough Law on Online Privacy." *The New York Times*, January 24, 2012, sec. Technology. https://www.nytimes.com/2012/01/24/technology/europe-weighs-a-tough-law-on-online-privacy-and-user-data.html.

U.S. Constitution, amend. 4.

Zomorodi, Manoush. "Do You Know How Much Private Info You Give Away Every Day?" TIME, March 29, 2017. https://time.com/4673602/terms-service-privacy-security/.

Cases Cited

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

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

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