American University Business Law Review

Volume 13 | Issue 2 Article 5

2024

The Domestic and International Limitations of the Third-Party Doctrine in the Digital Age

Miguel E. Serrano
ms1827a@american.edu

THE DOMESTIC AND INTERNATIONAL LIMITATIONS OF THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE

MIGUEL E. SERRANO*

I. INTRODUCTION

> Crime scene photography was well established in Anglo-American courts; and while the turn to filmic proof was perhaps a logical extension of available technology, it nevertheless marked a wholly new method of documenting criminality . . . [T]his straightforward ambition, however, yielded less than straightforward results.[1]

* J.D., American University Washington College of Law, 2024; B.A. 2019, University of Florida. Thanks to Professors Andrew Ferguson and Alex Joel for their instruction and scholarship, and the members of the *American University Business Law Review*.

1. Lawrence Douglas, *Film as Witness: Screening Nazi Concentration Camps Before the Nuremberg Tribunal*, 105 YALE L.J. 449, 451, 453 (1995).

Privacy and security move in tandem, like the twin feet of a compass.[2] Developments in privacy law protect confidential information in a technologically sophisticated world; and cybersecurity prevents sophisticated bad actors from accessing personal data.[3] These interests pair well, trace back centuries, and have catalyzed the evolution of the law around them.[4] Unfortunately, the third-party doctrine brings the natural tug and pull between these interests to a dead end.[5]

The third-party doctrine tells a story of U.S. privacy law falling behind in the digital landscape.[6] For one, the third-party doctrine pre-dates the internet by nearly a decade.[7] Yet the doctrine enables law enforcement, in most

2. *See* Paul R. Pillar, *The Pendulum of Opinion on Security and Privacy*, BROOKINGS INST. (June 11, 2013), https://www.brookings.edu/articles/the-pendulum-of-opinion-on-security-and-privacy/ ("[G]overnment agencies that are the target of recriminations at one time for not doing enough [for security] . . . are the target of recriminations for doing too much of the same thing [against privacy].").

3. Alexander W. Joel, *Choosing Both: Making Technology Choices at the Intersections of Privacy and Security*, 88 TEX. L. REV. 1751, 1752 (2010) ("Calls for the IC to make better use of technology are not uncommon, nor are complaints about its failure to capitalize on the latest technological developments . . . [and] [s]uch calls often raise concurrent concerns about the civil liberties and privacy implications of placing powerful new capabilities in the hands of intelligence operatives.").

4. *See* Remarks by the President on Review of Signals Intelligence, 2014 PUB. PAPERS 38, 38 (Jan. 17, 2014) ("Throughout American history, intelligence has helped secure our country and our freedoms[:] [i]n the Civil War, Union balloon reconnaissance tracked the size of Confederate armies by counting the number of campfires[;] [i]n World War II, code-breakers gave us insights into Japanese war plans and . . . intercepted communications helped save the lives of [American] troops[;] the National Security Agency . . . [gave] insights into the Soviet bloc . . . [But] even the United States proved not to be immune to the abuse of surveillance[:] . . . [the] government spied on civil rights leaders and critics of the Vietnam War[, and] in response to these revelations, additional laws were established in the 1970s to ensure that our intelligence capabilities could not be misused against our citizens.").

5. *See* Marguerite Rigoglioso, *Civil Liberties and Law in the Era of Surveillance*, STAN. LAW. MAG., Fall 2014, at 3 ("[T]he incredible evolution in technology over the past two decades has revolutionized both the tools available to the government for surveillance and those used by individuals to live their lives.").

6. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1539 (2000) ("[C]urrent privacy laws in the United States make up at best a thin patchwork, one that is plainly inadequate to meet the challenge of new data acquisition technologies.").

7. RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 3 (2014) ("[B]efore the advent of modern communications, government officials could not simply subpoena an Internet Service Provider (ISP), or Amazon, or Google for information relating to a target of investigation, but had to enter the suspect's home or office, sometimes by force, to retrieve personal information directly themselves.").

circuits, to acquire all sorts of evidence originating from cell phones, smart cars, internet browsing history, communications via apps, and wearable devices without a warrant.[8] Now that technology is essential for basic functions in day-to-day life, the doctrine cuts off an individual's expectations of privacy as soon personal data is collected by commercial entities.[9] Moreover, in the absence of federal legislation, the Supreme Court has not recognized citizen's rights to digital privacy.[10] While the advent of the third-party doctrine was a response to technological advances in the 1970s, since then, technology has vastly surpassed the doctrine's initial scope.[11]

Collection measures can routinely reach personal contacts, timestamps, and physical and electronic addresses because such information is regularly turned over to third-party companies.[12] This turnover also extends to web-browsing records, styles of traveling, eating, and behaving; refined Internet of Things devices ("Iot") can now capture gesture, habit, manners and customs, conversations, movement, and location.[13]

---

8. *See id*. at 13 (recognizing that the Ninth Circuit permits the third-party doctrine for internet service providers while the Sixth Circuit requires a warrant to access modern forms of communication).

9. *See* Michael Bahar et al., *The Third-Party Party-Crashing? The Fate of the Third-Party Doctrine*, LAWFARE (Oct. 19, 2017), www.lawfaremedia.org/article/third-party-party-crashing-fate-third-party-doctrine (questioning how the third-party doctrine has kept up with modern communication); *see also* Maryland v. Smith, 442 U.S. 735, 749 (Marshall, J., dissenting) (stating that the third-party exception is built around the suspension of disbelief for plain necessities: "[E]ven assuming that individuals 'typically know' that a phone company monitors calls" they must forgo "what for many has become a personal or professional necessity, [or else] accept the risk of surveillance").

10. THOMPSON II, *supra* note 7, at 23 (viewing Congressional privacy protections as weaker than the Fourth Amendment warrant requirement).

11. Cristina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age: Carpenter v. United States and the Fourth Amendment's Third-Party Doctrine*, 28 CATH. U. J.L. & TECH. 89, 91–92 (2020) ("Technological advancements and the proliferation of third-party records since the doctrine's inception in two Supreme Court decisions in the late 1970s raise questions about the stability of this doctrine in modern society.").

12. *See* Kenneth Olmstead & Michelle Atkinson, *Apps Permissions in the Google Play Store*, PEW RSCH. CTR. (Nov. 10, 2015), www.pewresearch.org/internet/2015/11/10/apps-permissions-in-the-google-play-store/ (listing the types of information given to third parties); *see also* Press Release, Fed. Trade Comm'n, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), www.ftc.gov/news-events/news/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived-consumers (discussing FTC actions against businesses that fail to disclose unfettered sharing of private consumer information).

13. *See* Patrick McFadin, *Internet of Things: Where Does the Data Go?*, WIRED, https://www.wired.com/insights/2015/03/internet-things-data-go/ (last visited Mar. 17, 2024) (discussing how IoTs gather large quantities of information about private

At the same time, the European Union ("EU") tells a different story, one of heightened privacy rights despite the massive data storage capabilities of third-party companies.[14] The EU's General Data Protection Regulation ("GDPR") affirmatively protects the right to privacy, provides European users with control of their personal data, and empowers consumers to dictate how personal information is stored by companies.[15] Even so, U.S. officials have levied criticisms against EU laws for disrupting the digital economy.[16] In the most prominent sign of this new era, concerns that U.S. privacy law lagged behind fundamental EU data rights culminated in the landmark decision *Data Protection Commission v. Facebook Ireland*,[17] ending an arrangement that allowed over 5,000 major companies to conduct business across the transatlantic market.[18]

In 2020, the Court of Justice of the European Union ("CJEU") invalidated Privacy Shield — the trade agreement between the EU and U.S., permitting data transfers between the regions — thus dissolving market relations with Europe's largest trading partner.[19] The CJEU held that legal mechanisms

---

activities, preferences, and habits).

14. *See, e.g.*, Mark MacCarthy, *The European Data Protection Board (EDPB) Goes After Tech's Personalized Ad Business Model*, BROOKINGS INST. (Feb. 1, 2023), www.brookings.edu/articles/the-european-data-protection-board-goes-after-techs-personalized-ad-business-model/ (stating that Meta was fined €390 million ($414 million) for violating Europe's General Data Protection Regulation after not bringing data processing operations into compliance).

15. Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 2, 12 [hereinafter GDPR].

16. *See* Peter P. Swire & Robert E. Litan, *Avoiding a Showdown Over EU Privacy Laws*, BROOKINGS INST. (Feb. 1, 1998), brookings.edu/articles/avoiding-a-showdown-over-eu-privacy-laws/ ("Other officials, such as those who are pushing Europe to be active in electronic commerce[,] . . . are thus wary of moves that could inhibit data flow into and out of the EU . . . . Others may claim that the Europeans could never enforce any data restrictions.").

17. Case C-311/18, ECLI:EU:C:2020:559 (2020).

18. Andrea Vittorio, *Legal Questions Loom Over Latest Trans-Atlantic Data Flows Deal*, BLOOMBERG L. (Oct. 11, 2022, 5:05 AM), https://news.bloomberglaw.com/privacy-and-data-security/legal-questions-loom-over-latest-trans-atlantic-data-flows-deal ("Questions surrounding the EU-US. data transfer regime have left companies such as Meta Platforms Inc.'s Facebook and Alphabet Inc.'s Google in legal limbo.").

19. THE CJEU JUDGMENT IN THE SCHREMS II CASE, at 2, PE 652.073 (Sep. 15, 2020) ("EU companies can no longer legally transfer data to the US based on the Privacy Shield framework. Companies that continue to transfer data on the basis of an invalid mechanism risk a penalty of €20 million or 4 % of their global turnover, pursuant to Article 83(5)(c) GDPR."). *See generally* CONG. RSCH. SERV., R47095, U.S.-EU TRADE

under the Privacy Shield, the Foreign Intelligence Surveillance Act ("FISA"), and Executive Order 12333 failed to provide adequate protections to EU citizens' data rights.[20] The CJEU held that data transfers to non-EU nations must meet equivalent data protection standards that users receive in the EU.[21] Ultimately, the ruling invalidated a $7.1 trillion transatlantic partnership between the U.S. and the EU.[22]

In response, the Biden Administration issued Executive Order 14086 in October 2022, in hopes of restoring market relations between the two largest democratic regions in the world.[23] As things stand, conflicting views on privacy rights may sunder U.S.-based companies from seamlessly operating in extraterritorial EU markets, resulting in a rift between major democracies in the digital age.[24] Alternatively, the social and economic advantages of low-cost, seamless, and worldwide communication should not overshadow the growth of illegal activity using the same means.[25] The United States is

---

RELATIONS 11 (2022) [hereinafter R47095, TRADE RELATIONS].

20. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems, ECLI:EU:C:2020:559 ¶ 201 (July 16, 2020) (holding the Privacy Shield Decision invalid). The Foreign Intelligence Surveillance Act prescribes rules for collecting foreign intelligence information in the United States but also dictates rules for targeted surveillance of foreign persons located outside the United States under Section 702. *See* Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–62 (2000 & Supp. II 2002)). The President's authority to issue Executive Orders comes from the vesting clause in Article II. U.S. CONST. Art. II § 1 (stating that "[t]he executive Power shall be vested in a President of the United States of America"). Executive Order 12333 allows the NSA to collect, retain, analyze, and disseminate foreign signals intelligence information by foreign persons outside the United States. *See* Exec. Order No. 12,333, 3 C.F.R. § 200 (1982).

21. *See Data Prot. Comm'r, supra* note 20 (requiring appropriate safeguards by non-EU countries to be essentially equivalent to the EU standards).

22. R47095, TRADE RELATIONS, *supra* note 19.

23. *See FACT SHEET: President Biden Signs Executive Order to Implement the European Union–U.S. Data Privacy Framework*, WHITE HOUSE (Oct. 7, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ [hereinafter WHITE HOUSE] ("[T]he United States will take [steps] to implement . . . [its] commitments under the European Union-U.S. Data Privacy Framework . . . [to restore] [t]ransatlantic data flows[,] . . . critical to enabling the $7.1 trillion EU-U.S. economic relationship . . . [and] restor[ing] an important legal basis for transatlantic data flows.").

24. Alex Joel, *Protect Privacy. That's an Order.*, LAWFARE (Apr. 6, 2021, 1:09 PM), https://www.lawfaremedia.org/article/protect-privacy-thats-order ("[U]nderneath the complexity of [the U.S. legal] framework and . . . European partners is a shared commitment to conducting intelligence to pursue legitimate aims in a democratic society, under the rule of law, while respecting fundamental rights and freedoms.").

25. *See generally* OFF. DIR. NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 24 (2022) (outlining how emerging technologies can

now on notice: the state of privacy, security, and economic maturity are each at stake in the digital future.

This Comment argues that the third-party doctrine further alienates EU-U.S. partnerships because the doctrine subverts privacy interests as binding legal precedent. Part II will explore the history of the third-party doctrine up until the *Carpenter* decision and explain why U.S. privacy rights are linked with access to third-party information. This Comment will further outline EU data protection laws, EU legislation, and the CJEU's *Schrems II* decision. In Part III, this Comment will also analyze the new data protection framework, Executive Order 14086, and discuss whether it fails to overcome the CJEU's concerns over U.S. privacy laws for EU subjects. By comparing *Carpenter* to the *Schrems II* decision, this Comment will gauge what steps are needed to reconcile the third-party doctrine with EU standards. Finally, Part IV of this Comment will recommend that Congress codify privacy rights for U.S. citizens modeled after the GDPR, or alternatively, offer an updated test for data protection under the law.

II. THE EVOLUTION OF PRIVACY RIGHTS AND DATA PROTECTION LAW IN THE U.S. AND EU

> Being able to transfer data across borders is fundamental in this digital era for everything from social media use to international trade and cooperation on global health issues. Yet, without common principles and safeguards, the sharing of personal data across jurisdictions raises privacy concerns, particularly in sensitive areas like national security.[26]

The principles of European and U.S. privacy law, both stemming from the same history, are not mutually exclusive.[27] The two legal systems share values that adhere to democratic principles.[28] However, as of now, privacy norms across both regions have diverged.[29] There is no comprehensive data

---

disrupt and destabilize the American security apparatus).

26. *Landmark Agreement Adopted on Safeguarding Privacy in Law Enforcement and National Security Data Access*, OECD (Dec. 14, 2022), https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm (internal quotations omitted).

27. *See* Joel, *supra* note 24 (finding a shared commitment in principles of the U.S. and EU privacy frameworks).

28. *See id*. (recognizing the U.S. and its European partners as agreeing to follow the rule of law in its respective democratic societies).

29. *See*, *e.g.*, NIR KSHETRI, THE QUEST TO CYBER SUPERIORITY 76 (Springer, 2016) (discussing how differences in privacy legislation have disrupted U.S. companies' international trade and raised barriers to EU companies' international trade); Paul M.

protection in U.S. law, unlike in Europe.[30] The scope of European data rights is much broader than those in the U.S.[31] Moreover, the U.S. has pushed for tougher security laws at the expense of individual privacy,[32] whereas Europe has upheld the right to privacy even against other fundamental rights, such as freedom of expression.[33]

Over time, these differences have steadily eroded a market between the U.S. and EU, the seamless exchange of information that serves fraud prevention networks, cloud computing, financial services, e-commerce, education, research, telecommunication, and streaming and entertainment.[34] Contrasting views on privacy have placed obstacles before companies

---

Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1823, 1874 (2011) (explaining that information privacy in the United States lacks a uniform definition whereas the information privacy is codified and defined in the European Union's privacy laws); Keith Bradsher & Katrin Bennhold, *World Leaders at Davos Call for Global Rules on Tech*, N.Y. TIMES (Jan. 23, 2019), https://www.nytimes.com/2019/01/23/technology/worldeconomic-forum-data-controls.html (quoting multiple world leaders calling for more universal standards on personal data privacy protection); Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1978 (2013) (outlining the differences in their paths of regulating information privacy between the U.S. and EU); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1155 (2004) (remarking that the United States and Western Europe's privacy conflicts "reflect unmistakable differences in sensibilities about what ought to be kept private").

30. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ ("The United States doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA.").

31. Charter of Fundamental Rights of the European Union, arts. 7, 8, Mar. 3, 2010, 2010 O.J. (C 83) 389, 393 [hereinafter The Charter].

32. *See, e.g.*, Sarah Lamdan, *When Westlaw Fuels Ice Surveillance: Legal Ethics in the Era of Big Data Policing*, 43 N.Y.U. REV. L. & SOC. CHANGE 255, 263 (2019) ("After the September 11, 2001, terrorist attacks, national security concerns trumped due process considerations and the U.S. surveillance regime exploded from individualized to mass surveillance[.] The Patriot Act, passed shortly after the attacks, amended [FISA] and empowered federal agents to use new, more invasive surveillance tactics.").

33. *See* Rolf H. Weber, *On the Search for an Adequate Scope of the Right to Be Forgotten*, 6 JIPITEC 2, 3 (2015) (discussing the holding in *Google Spain*, where the CJEU held that "an individual has the right to request that his or her personal data be removed from accessibility via a search engine," and the subsequent 200,000 erasure requests filed with Google).

34. *See generally* Center for Information Policy Leadership, *The "Real Life Harms" of Data Localization Policies* (Discussion Paper No. 1, 2023) (discussing the economic dangers and business impact of data localization policies).

operating in both markets, and previous EU-U.S. transatlantic agreements have not cured these jurisprudential differences.[35]

A. Privacy Rights in the United States

In the United States, digital information is subject to threats from rival governments and international criminal entities.[36] However, when U.S. laws and regulations have targeted these bad actors in the name of public safety and national security, it has come at the expense of liberty interests.[37] The right to privacy goes out imperceptibly when no countervailing power checks national security objectives.[38] In various contexts, data is tracked and stored by private industries and can later be retrieved by law enforcement and federal agents in criminal investigations.[39] Privacy advocates link the U.S.

---

35. *See generally* Shanzay Pervaiz, *Is the Schrems II Ruling One of the "Most Significant Risks" Facing U.S. Companies?*, PRIVACY ACROSS BORDERS (Mar. 23, 2017), https://privacyacrossborders.org/2022/03/23/is-the-schrems-ii-ruling-one-of-the-most-significant-risks-facing-u-s-companies/.

36. *See, e.g.*, *America is Under Cyber Attack: Why Urgent Action Is Needed: Hearing Before the H. Subcomm. on Oversight, Investigation And Mgmt. of the H. Comm. on Homeland Sec.*, 112 Cong. 1 (2022); *see also* Laura Clark Fey & Sarah D. Wiese, *American the Vulnerable: The Nation State Hacking Threat to Our Economy, Our Privacy, and Our Welfare*, 30 KAN. J.L. & PUB. POL'Y 370, 375 ("Nation states are widely believed to be behind many of the high-profile data breaches and cybersecurity incidents in the last decade."); *The Growing Threat of Cyberattacks*, THE HERITAGE FOUND. (2021), https://www.heritage.org/cybersecurity/heritage-explains/the-growing-threat cyberattacks#:~:text=Key%20Takeaways,the%20country's%20diverse%20cyber%20networks.

37. *See* Carroll Doherty, *Balancing Act: National Security and Civil Liberties in Post-9/11 Era*, PEW RSCH. CTR. (June 7, 2013), https://www.pewresearch.org/short-reads/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/ (citing a poll regarding how Americans have found it necessary to give up civil rights to curb terrorism).

38. Katz v. United States, 389 U.S. 347, 350 (1967) (Harlan, J., concurring) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"); *see also* Mark Silverstein, *Privacy Rights in State Constitutions: Models for Illinois?*, 1989 U. ILL. L. REV. 215, 215 n.6 ("[T]he federal Constitution[] contain[s] only an implied right of privacy[, and] . . . state constitutional rights of privacy are stronger than the federal Constitution's."); Kristen M. Hadgis et al., *Data Privacy: Evolving Updates to the Global Landscape*, MORGAN LEWIS (Sept. 14, 2022), https://www.morganlewis.com/pubs/2022/09/data-privacy-evolving-updates-to-the-global-landscape (explaining that while the U.S. does not have a federal privacy law, new privacy legislation in California, Virginia, Colorado, Utah, and Connecticut will take effect in 2023).

39. *See* Thomas Brewster, *Meet The Secretive Surveillance Wizards Helping The FBI And ICE Wiretap Facebook And Google Users,* FORBES (Feb. 23, 2022, 1:53 PM), https://www.forbes.com/sites/thomasbrewster/2022/02/23/meet-the-secretive-surveillance-wizards-helping-the-fbi-and-ice-wiretap-facebook-and-google-users/?s&sh=34cd216d3f0f ("[Law enforcement requests] reveal[] . . . just how [much]

system to one of decreasing constitutional protections when it comes to how data is collected, used, and shared.[40]

Katz v. United States[41] is a landmark Supreme Court case for the right to privacy, creating the "reasonable expectation of privacy" test.[42] The issue was whether the Fourth Amendment applied to police eavesdropping in a private booth.[43] Consistent with the historic pattern of criminal investigations at the time, federal agents eavesdropped on Charles Katz while he used a public payphone booth to illegally transmit gambling information across state lines.[44] Attaching an electronic listening and recording device to the outside of the booth, the government argued that the recording technology was constitutional[45] because there was no need to physically search or seize Katz's property.[46] The Supreme Court disagreed, holding that the action threatened Katz's privacy interest in the conversation itself.[47] Ultimately, the Court held that the government's use of a listening device constituted a warrantless search under the Fourth Amendment.[48] A

---

tech providers such as Apple, Facebook and Google provide information to police when they're confronted with a valid warrant or subpoena."); *see also* Nathaniel Kim, *The Impact of Public-Private Data Sharing on Law Enforcement*, GEO. L. TECH. REV. (Apr. 2022), https://georgetownlawtechreview.org/the-impact-of-public-private-data-sharing-on-law-enforcement/GLTR-04-2022/ ("These [data brokers] have begun buying data from private companies and then reselling it to [law enforcement].").

40. Kim, *supra* note 39 (describing the creation of surveillance capitalism); *see also* Julie E. Cohen, Essay, *How (Not) to Write a Privacy Law*, COLUM. KNIGHT FIRST AMEND. INST. (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law ("In many legal systems—most notably, those in European Union member states—disclosure of personal information for law enforcement or national security purposes doesn't eliminate the need to comply with data protection obligations . . . [but u]nder the U.S. approach, law enforcement and national security exceptions tend to move the activity beyond the reach of data protection obligations altogether.").

41. 389 U.S. 347 (1967).

42. *Id.* at 353, 361 (Harlan, J., concurring) (formulating a two-pronged test to determining whether the privacy interest is paramount: "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'").

43. *Id.* at 351 ("[T]he Fourth Amendment protects people, not places.").

44. *Id*. at 349.

45. *See Katz v. United States (1967)*, NAT'L CONST CTR., https://constitutioncenter.org/the-constitution/supreme-court-case-library/katz-v-united-states (last visited Mar. 13, 2024) ("As public phone booths and electronic communications became more common in American life, the Supreme Court had to determine whether and how to apply a constitutional text written in 1791 to the technological changes of modern life.").

46. *Katz*, 389 U.S. at 350.

47. *Id.* at 351.

48. *Id*. at 353.

public payphone conversation was not a mere misdeed; rather, Katz's subjective belief that he would not be overheard and society's objective expectations to be heard in private were meaningful considerations for the court.[49] While the third-party doctrine is a response to rapid technological innovation, even early on, the Supreme Court was equally aware of privacy interests inherently tied to developments in technology.[50]

The principles that underscored the third-party doctrine differ from those animating the law today. In *United States v. Miller*[51], the Supreme Court did not uphold Fourth Amendment protections when an individual's bank records were seized by the government without a warrant.[52] Jack Miller was charged with transporting illegal whiskey in violation of the National Prohibition Act, and a key part of the government's investigation was reviewing Miller's bank records, which they seized without a warrant.[53] Acknowledging purported privacy concerns, the Supreme Court nonetheless reasoned that Miller did not have a privacy interest in records voluntarily given over to the bank.[54] The ruling emerged as a crux for creating the third-party doctrine: a person lacks reasonable expectation of privacy to information voluntarily provided to another.third party. [55] Soon after, the doctrine was expanded to other methods of police surveillance, which was not contemplated by paper banking records nearly fifty years ago.[56]

Three years later, the Supreme Court promulgated the third-party doctrine in *Smith v. Maryland*.[57] The Court addressed the issue of whether the Fourth Amendment protected an individual's phone records from a warrantless

---

49. *Id*. at 351–52.

50. *But see* Margaret Hu, *Cybersurveillance Intrusions and the Evolving Katz Privacy Test*, 55 AM. CRIM. L. REV. 127, 129 (2018) ("Technological developments, however, may change which expectations of privacy are 'reasonable,' calling the continued viability of the *Katz* 'reasonable expectation of privacy' test into question.").

51. 425 U.S. 435 (1976).

52. *Id.* at 455.

53. *See id*. at 439–40.

54. *See id.* at 440.

55. *See* THOMPSON II, *supra* note 7, at 1 ("[T]he Court held that a customer has no reasonable expectation of privacy in . . . checks and deposit slips he gives to his bank [], as he has exposed them to another and assumed the risk they could be handed over to the government.").

56. *See* Cristina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age:* Carpenter v. United States *and the Fourth Amendment's Third-Party Doctrine*, 28 CATH. U. J.L. & TECH. 89, 97 (2020) ("*Miller* . . . preceded the rise of mass digital information aggregation, and, since [*Miller*], there has been a surge of data collection and processing."); *see also* Carpenter v. United States, 585 U.S. 296, 316 (2018) ("We do not disturb the application of *Smith* and *Miller*").

57. 442 U.S. 735, 744 (1979).

seizure.[58] In the case, Michael Lee Smith, a suspect of an investigation into harassing phone calls, was arrested after police obtained his call records from the local phone company.[59] Using a pen register, the police traced the suspicious calls back to Smith's phone.[60]

Smith asserted a privacy interest in the phone numbers from his personal registry, but the third-party doctrine precluded Smith's claim.[61] The Supreme Court ultimately held that an individual does not have a reasonable expectation of privacy to dialed phone numbers once they are voluntarily provided to a phone company.[62]

The doctrine evolved to touch and concern a plethora of new information that persons share with companies, giving law enforcement access without a warrant.[63] Since its origin in the 1970s, the third-party doctrine has been a cornerstone in law enforcement efforts to investigate crimes.[64] Law enforcement use the third-party doctrine to access personal information routinely given to commercial companies.[65] With cybercriminals, for example, the third-party doctrine enables law enforcement to access cyber activity from the onset of a server breach.[66] By having quick access to this

58. *See id.* at 736.

59. *See id.* at 737.

60. *See id.*

61. *See* Tonja Jacobi & Dustin Stonecipher, *A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance*, 97 NOTRE DAME L. REV. 823, 834 (2022) ("[*Miller* and *Smith*] laid the groundwork for a per se third-party doctrine that is ill-suited for our modern information-sharing age.").

62. *See id.* at 835 (quoting *Smith*, 442 U.S. at 744–45).

63. *See* THOMPSON II, *supra* note 7, at 9.

64. *See id.* at 12 ("After *Miller* and *Smith*, the courts have applied the third-party doctrine to a host of various scenarios including metadata connected to Internet communications, cell phone location information, and utility billing records, among others.").

65. *See id.* at 16 ("As a more practical matter, assistance from third parties is utilized by law enforcement in almost every investigation. When investigating a murder, robbery, or any other crime committed in the real world . . . . To conduct these interviews, [] officers generally need not obtain a warrant, and witnesses who refuse to cooperate can be compelled to testify with a grand jury subpoena.").

66. *See, e.g.*, Sean Hollister, *Colonial Pipeline Reportedly Paid the Hackers Nearly $5 Million, Despite Suggestions to Contrary*, THE VERGE (May 13, 2021, 1:09 PM), https://www.theverge.com/2021/5/13/22434381/colonial-pipeline-darkside-hacker-ransomware-ransom-oil; Dan Goodin, *Hackers Access Security Cameras Inside Cloudflare, Jails, and Hospitals*, ARS TECHNICA (Mar. 10, 2021, 12:14 AM), https://arstechnica.com/information-technology/2021/03/hackers-access-security-cameras-inside-cloudflare-jails-and-hospitals/; Samantha Schwartz, *Security Flaws Enabled Tampa-Area Water Utility Hack*, SMART CITIES DIVE (Feb. 12, 2021), https://www.smartcitiesdive.com/news/water-supply-cyber-attack-tampa-florida-ics-security/594845/; Kevin Collier, *Hackers Release Personal Info of 22 D.C. Police*

digital information, law enforcement can rapidly investigate, track down, and prosecute criminals.[67]

However, with the rise of globalization, increased sharing of data across borders, and the exponential use of digital tools, the third-party doctrine's analog origins are at odds with abundance of information today.[68] As a result, civil liberties groups and digital privacy advocates argue that giving the government free access to copious amounts of personal information on third-party servers, apps, and websites is an obvious point of private ingress that violates the Fourth Amendment.[69]

Although *Miller* and *Smith* have remained a salient feature of the legal landscape since 1976, the categorical force of these rulings came into question in *Jones v. United States*.[70] In 2012, Antoine Jones was suspected of operating a drug trafficking organization.[71] Law enforcement installed a GPS tracking device beneath Jones' Jeep Grand Cherokee pursuant to a District of Columbia warrant, but the device was actually installed when the vehicle was in Maryland, outside the warrant's jurisdiction.[72] The issue the Court faced was whether "2000 pages of location-information data"

Officers, NBC NEWS (May 11, 2021, 2:30 PM), https://www.nbcnews.com/tech/security/hackers-release-personal-info-22-dc-police-officers-rcna897.

67. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 601 (2009) ("Critics have often focused on powers of the government to harass innocent individuals . . . . But the Justices of the Supreme Court do not have this luxury. They must create rules that apply for investigations of both the innocent and the guilty in a world . . . . They must look systemically to generate a set of rules that will apply to both.").

68. *See* Johana Bhuiyan, *How Can US Law Enforcement Agencies Access Your Data? Let's Count the Ways*, GUARDIAN (Apr. 4, 2022, 10:05 AM), https://www.theguardian.com/technology/2022/apr/04/us-law-enforcement-agencies-access-your-data-apple-meta ("Google, for example, received more than 39,000 requests for user information between July and December 2020, according to the company's most recent transparency report. Google handed over user info in response to more than 80% of those requests, affecting the accounts of more than 89,000 users.").

69. *See* Rachel Levinson-Waldman & Alexia Ramirez, *Cell Phone Privacy at the Supreme Court*, BRENNAN CTR. FOR JUST. (June 7, 2018), https://www.brennancenter.org/our-work/analysis-opinion/cell-phone-privacy-supreme-court; *see also* Jennifer Safstrom, *The Right to Keep Personal Data Private:* Carpenter v. U.S., ACLU (Sept. 15, 2017), https://www.aclu.org/news/privacy-technology/right-keep-personal-data-private-carpenter-v-us.

70. *See* United States v. Jones, 565 U.S. 400, 406 (2012); *supra* notes 18–19 (accompanying text).

71. *Id.* at 402, 413.

72. *Id.* at 402–03.

regarding Jones' movements for four weeks were acquired unconstitutionally,outside of the warrant's bounds.[73]

Jones argued that the GPS tracking device constituted a warrantless search in violation of the Fourth Amendment.[74] Harkening back to *Katz*, the Supreme Court reasoned that Jones retained an expectation of privacy in his physical movements; moreover, applying a GPS tracking device to monitor his vehicle's movements was a physical intrusion of his property interest without a warrant.[75] Focusing on the issue of Jones' collected movements, the Supreme Court generally agreed with his argument, holding that the Fourth Amendment protects an individual's physical movements from being tracked by the government.[76] However, the Court distinguished Jones from cases where users voluntarily provided location data without any police intervention, thus "abrogat[ing] the need for technological intrusions into physical property."[77] For comparison, individuals routinely share location data with smart phones, apps, and devices connected to geofencing and geolocation operations.[78] The collection of location data occurs on various fronts, but the Supreme Court looked specifically to data collection from cell-site towers.

Carpenter v. United States[79] was the first Supreme Court decision in decades to balk before an opportunity to extend the third-party doctrine once again.[80] The case addressed the issue of whether the Fourth Amendment

---

73. *See* Benjamin J. Priester, *Five Answers and Three Questions After* United States v. Jones *(2012), the Fourth Amendment "GPS Case*,*"* 65 OKLA. L. REV. 491, 494 (2013) ("[T]he four-week log of Jones's public movements . . . establish[ed] his connections to various locations and individuals involved in the conspiracy."); *see also Jones*, 565 U.S. at 402.

74. *Jones*, 565 U.S. at 403.

75. *See id.* at 405–07.

76. *Id*.

77. *See* Priester, *supra* note 73, at 501 ("Consequently . . . the police would have no need to examine the physical smartphone itself when they could readily acquire the identical backup contacts list maintained by Android's Gmail or Apple's iCloud synergies.").

78. *See* Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

79. 585 U.S. 296 (2018).

80. *See* LAURA HECHT-FELELLA, THE FOURTH AMENDMENT IN THE DIGITAL AGE: HOW *CARPENTER* CAN SHAPE PRIVACY PROTECTIONS FOR NEW TECHNOLOGIES 3 (2021); *see also* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019) (lauding *Carpenter* for strengthening privacy protections); Orin S. Kerr, *First Thoughts on* Carpenter v. United States, REASON: THE VOLOKH CONSPIRACY (June 22, 2018, 12:20 PM), https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-

prevents the government from obtaining an individual's cell phone location records without a warrant, and in a narrow fashion, the Court affirmed constitutional safeguards.[81]

In the case, law enforcement connected Timothy Carpenter to several armed robberies based on cell phone location records acquired from his cell phone provider without a warrant.[82] The government relied on *Smith* and *Miller* to argue that Carpenter had no expectation of privacy regarding the location data that he provided to his cell phone carrier.[83] But the Court disagreed, holding that the government had violated Carpenter's Fourth Amendment right.[84]

First, the Court stated that an individual possesses a reasonable expectation of privacy in their location records, like in *Jones*.[85] Second, the Court distinguished the extent to which *Smith* and *Miller* could be applied to cell phone towers, which collect data without any affirmative acts by the user.[86]

Put differently, *Carpenter* ushered privacy rights away from the third-party doctrine.[87] From a public policy perspective, the 2010s were shocked by Edward Snowden's 2014 disclosure of the National Security Agency's ("NSA") collection program and the intelligence community's surveillance practices, which turned public attention toward government data collection.[88]

---

united-sta/ (noting the Chief Justice's criticism of the third-party doctrine's slippery slope).

81. *Carpenter*, 585 U.S. at 303.

82. *Id.* at 301–02.

83. *See id.* at 297.

84. *Id.* at 297, 320.

85. *Id.* at 309–10.

86. *Id.* at 311.

87. *See, e.g.*, HECHT-FELELLA, *supra* note 80, at 30 ("As technological advances have fundamentally changed what society views as private and how we store information . . . *Carpenter* should be read broadly as reimagining what a reasonable expectation of privacy in the digital age is."); Sarah Murphy, Note, *Watt Now?: Smart Meter Data Post*-Carpenter, 61 B.C. L. REV. 785, 809–15 (2020) (preventing the third-party doctrine from applying to smart meter data); Tonja Jacobi & Dustin Stonecipher, *A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance*, 97 NOTRE DAME L. REV. 823, 828, 889–91 (2022) (discussing the public health danger of the Third-Party Doctrine following the COVID-19 Pandemic with the proliferated use of contact tracing apps, Bluetooth-enabled devices, anonymized location data, and movement trends).

88. *Catalog of the Snowden Revelations*, LAWFARE (Jan. 22, 2014, 1:00 AM) (providing a timeline of Snowden's disclosure of NSA classified information, including: the PRISM collection program; the practice of upstream collection and collection of bulk telephony metadata for both U.S. and non-U.S. citizens; and surveillance of foreign government leaders).

Suddenly, millions of U.S. citizens accused the government of turning cell phones into tracking devices,[89] prompting Congress to pass the USA Freedom Act in 2015[90] and allow Section 215 of the Patriot Act to expire.[91]

However, the Supreme Court's decision in *Carpenter* was narrowly confined to the facts in that case.[92] *Carpenter* does not identify the boundaries of the third-party doctrine, and there is sufficient reason to doubt the viability of U.S. privacy rights as more mature forms of location-based data emerge; third-party vendors begin to share data with fourth parties; and 5G networks, biometric data, and autonomous technology proliferate the consumer market.[93]

---

89. *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RSCH. CTR. (Sept. 21, 2016), https://www.google.com/search?client=safari&rls=en&q=See+Lee+Rainie%2C+The+state+of+privacy+in+postSnowden+America%2C+PEW+RESEARCH+CENTER&ie=UTF-8&oe=UTF-8 (noting that "some 86% of Americans take steps to mask or remove their digital footprint, 91% of American adults believe consumers do not have control over how companies collect and use personal information, and "57% [of Americans say it is] unacceptable for the government to monitor the communications of U.S. citizens"); *see also* Safstrom, *supra* note 69.

90. H.R. 3361, 113th Cong. (2014). The USA Freedom Act was the United States' most significant surveillance reform since 1978, narrowing the U.S. intelligence community's discretion over intelligence gathering by prohibiting bulk collection, creating judicial review over the acquisition of data through the Foreign Intelligence Surveillance Court ("FISC"), amending the Foreign Intelligence Surveillance Act (FISA), and instituting mandatory reporting and transparency requirements.

91. *See* India McKinney, *Section 215 Expired: Year in Review 2020*, ELEC. FRONTIER FOUND. (Dec. 29, 2020), https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020 (discussing the end of the bulk telephone metadata program and the issues of it lapsing because lawmakers failed to reach an agreement about reform).

92. Carpenter v. United States, 585 U.S. 296, 316 (2018) ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not . . . call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.").

93. *See* Chris Ott, *Insight: Cracking Open a Can of Worms: Why* Carpenter v. United States *May Not Be the Privacy Decision that Was Needed . . . or Wanted*, BLOOMBERG L. (July 9, 2018) ("[T]he decision does little to assuage the growing modern privacy concerns increasingly focused on collection and sharing of data not by the government, but by private companies.").

B. Privacy Rights in the European Union

Whether it is internet, cellphone, social media networks, cloud software, or IoT device data, European Union law provides protections for user data.[94] By the 1980s, the EU was contemplating matters associated to rise of personal information, including its collection and use by businesses.[95] As a result, the EU emerged at the forefront of global privacy rights, becoming one of the most influential jurisdictions in the world for protecting internet users from excessive data collection and abuse.[96]

During the early days of the internet, EU law set a robust framework around the rights of users operating web-based services and created a strict set of rules for companies to abide by when dealing with user data.[97]

Initially, the EU's privacy protection was largely left to the individual Member States.[98] Then the Data Protection Directive was founded, laying basic and centralized principles for the protection of personal data.[99] This included the principle of proportionality — which ensured that data was collected only for the requested purposes — and the right to information and consent — which required companies to be transparent about collecting, storing, and using personal data.[100] At the turn of the century, the EU also

94. *See* Adam Satariano, *What the G.D.P.R., Europe's Tough New Data Law, Means for You*, N.Y. TIMES (May 6, 2018), https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html.

95. Chris Mirasola, *Summary: The EU General Data Protection Regulation*, LAWFARE (Mar. 1, 2018) ("These substantial protections build on a history of European concern for data privacy dating to 1980 . . . [and the European Commission's] recommendations carry real weight; as of [ ] first review, 2,400 U.S. companies have signed up for [ ] [compliance checks], including some of the largest U.S. tech firms (Google, Facebook and Microsoft).").

96. Paul M. Schwartz, *supra* note 29 ("The EU has played a major role in international decisions involving information privacy, a role that has been bolstered by the authority of EU member states to block data transfers to third party nations, including the United States.").

97. The Charter, *supra* note 31, at 389, 393 (enshrining the protection of individuals with regard to their personal data rights); GDPR, *supra* note 15, at 1 (governing and regulating by the Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC).

98. Council Directive 95/46/EC, 1995 O.J. (L 281); *see also* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 372 (2019) (requiring "each of the twenty-eight Member States to enact national legislation that protects 'the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'").

99. Rustad & Koenig, *supra* note 98.

100. *Id.*

adopted the Electronic Signatures Directive,[101] the E-Commerce Directive,[102] and the Electronic Communications Data Protection Directive.[103] These laws strengthened privacy rights when it came to communication and marketing data, provisions concerning rights to anonymity, and rules to protect against unsolicited communications and commercial surveillance.[104]

In 2018, the EU fully codified fundamental data rights by passing the General Data Protection Regulation.[105] The GDPR added rules on transparency obligations, drastically increased the fines for companies who failed to comply with data protection rules, and gave individuals robust rights to their data.[106] Moreover, the GDPR set out a much more detailed framework for data protection, including data minimization, data portability, the right to be forgotten, and the right to be informed.[107] The GDPR also provided "specific rules to ensure that [the] high level of data protection within the European Union [was guaranteed when] personal data is transferred to a non-EU state."[108] In other words, data can be transferred to a non-EU nation only if its extraterritorial laws comply with privacy standards set forth by the EU.[109] The EU's legal framework has been a catalyst for the development of modern privacy law; and the U.S. has had to respond because of the risk of transatlantic trade of information coming to a sharp end.[110]

GDPR regulations build upon rights enshrined in the EU's Charter of Fundamental Rights (the "Charter").[111] Article 8 provides that "[e]veryone

101. Council Directive 1999/93/EC, 2000 O.J. (L 013) 12–20.

102. Council Directive 2000/31/EC, 2000 O.J. (L 178) 1–16.

103. Council Directive 2002/58/EC, 2002 O.J. (L 201) 37–47.

104. *See* Adam Deakin, *GDPR: 10 Months To Go — A Short History of Data Protection*, VULTURE (July 2017) https://vutu.re/blog/gdpr-timeline-a-history-of-data-protection/.

105. *See* GDPR, *supra* note 15.

106. *See id.* at arts. 4–23.

107. *Id.*

108. *See id.* at arts. 45–50; *see also* Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party at 5. *See generally United States v. Microsoft Corp.*, 584 U.S. 236 (2018).

109. DLA Piper, *EU Data Protection Legislation Has Faced Huge Change*, https://www.dlapiper.com/en-us/insights/topics/gdpr (last visited June 12, 2024) ("Even if an organization is able to prove that it is not established within the EU, it is still be caught by GDPR if it processes [the] personal data of data subjects who are in the Union [and] the processing activities are related 'to the offering of goods or services' . . . to [European] data subjects . . . or 'the monitoring of their behavior[.]").

110. Pervaiz, *supra* note 35.

111. The Charter, *supra* note 31, at 389, 393.

has the right to the protection of personal data concerning him or her."[112] The Charter, combined with the GDPR, imbues data protection into the business landscape.[113]

Accordingly, on July 16, 2020, the Court of European Justice ("CJEU") issued *Schrems II* based on principles conferred by the GPDR and the Charter. [114] The decision effectively invalidated the EU-U.S. Privacy Shield.[115] The CJEU combined two cases.[116] First, a group of European privacy activists, named La Quadrature du Net, challenged Privacy Shield in European court.[117] At the same time, activist Maximillian Schrems sued Facebook in the Irish High Court by arguing that Standard Contractual Clauses ("SCCs")[118] under Privacy Shield did not confer data rights to EU data subjects.[119] Schrems argued that the U.S. intelligence community was just as likely to claim his Facebook data when transferred under SCCs — the pre-approved contractual clauses that enable U.S. companies to comply with EU data obligations — because the government could sidestep such clauses to obtain EU user's information.[120] The CJEU ultimately invalidated the transatlantic data framework and ruled out the main alternative transfer method of SCCs for failing to provide "essentially equivalent" protections.[121]

---

112. *Id.* (quoting art. 8).

113. *See* Mistale Taylor, *The EU's Human Rights Obligations in Relation to its Data Protection Laws with Extraterritorial Effect*, 5 INT'L DATA PRIV. L. 246, 247 (2015).

114. *Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems,* Case C-311/18, ECLI:EU:C:2020:559, at para. 201 (2020) [hereinafter *Schrems II*].

115. *Id*. at para. 134; Ian Brown & Douwe Korff, EXCHANGES OF PERSONAL DATA AFTER THE SCHREMS II JUDGMENT, EUR. PARL. COMM. ON CIV. LIBERTIES (2021) (stating "[t]he CJEU invalidated the Privacy Shield adequacy decision because FISA s.702 and E.O. 12333, even as limited by PPD-28, are too permissive to meet the GDPR's standards of necessity and proportionality and do not provide EU data subjects with effective judicial redress"); *see also Schrems II*, *supra* note 114, at para. 192.

116. *See* Schrems v. Data Prot. Comm'r, Case C-362/14, ECLI:EU:C:2015:650, at 28 (stating that in October 2015, the CJEU held in *Schrems v. Data Protection Commissioner* that Facebook's rules under U.S. privacy law did not confer rights of redress similar to the EU's Charter of Fundamental Rights and European privacy legislation).

117. *Schrems II*, *supra* note 114.

118. *See* Hadgis et al., *supra* note 34 (stating "In June 2021, the European Commission issued modernized SCCs that replaced [ ] SCCs . . . adopted under the previous Data Protection Directive 95/46" — the use of SCCs was an alternative method for data transfers from the European Union to third countries without adequacy decisions, but after December 27, 2022, organizations cannot lawfully rely on prior SCCs to transfer data to the United States and other countries without an adequacy decision).

119. *See id*.

120. *See id.*

121. *See id.*

On October 7, 2023, the Biden Administration signed Executive Order 14086 ("EO 14086") to resume the EU-U.S. transatlantic data flow.[122] According to its plan, "EO 14086's enhanced safeguards will . . . allow[] U.S. businesses that agree to abide by a set of privacy safeguards embodied in a new "EU-US Data Privacy Framework" (the DPF) to receive European personal data without continuing to engage in expensive and time-consuming alternative transfer mechanisms."[123]

III. HOW THE PRE-INTERNET "THIRD-PARTY DOCTRINE" FARES AMID RAPID ONLINE GLOBALIZATION

> Privacy is not a discrete commodity, possessed absolutely or not at all.
>
> Thurgood Marshall[124]

A. Cross-Atlantic Law: Comparing the "Rights of the Data Subject" After Carpenter

The *Schrems II* court formed the "essential equivalency" standard to evaluate EU-data transfers to countries outside the European Union.[125] First, non-EU data protection laws are compared to the GDPR and the Charter, which codify EU citizen's data rights.[126] Second, extraterritorial laws must provide essentially equivalent rights and remedies as those given by the GDPR for data protection and privacy.[127] The GDPR "recognizes that all 'natural persons' have a 'fundamental right' to 'the protection of their personal data.'"[128] Thus, the rules safeguard EU citizens because these principles exist when non-European companies process the data of European subjects.[129]

---

122. *See* WHITE HOUSE, *supra* note 23.

123. Michael Kleinman & Talia Bulka, *A Pessimist's Assessment of the Proposed EU-US Data Privacy Framework Under 'Schrems II*,*'* N.Y.L.J. (2022).

124. Smith v. Maryland, 442 U.S. 735, 749 (1979) (J. Marshall, dissenting).

125. *See Schrems II*, *supra* note 114, para. 248 ("[A]s the Court made clear in the judgment in *Schrems*, that standard does not mean that the level of protection must be 'identical' to that required in the Union. Although the means which a third country employs in order to protect the data subjects' rights may differ from those prescribed by the GDPR read in the light of the Charter, 'those means must . . . prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.'").

126. The Charter, *supra* note 31, art. 8.

127. GDPR, *supra* note 15, at 61; *see also Schrems II*, *supra* note 114, para. 89 ("[I] share the view that the validity of Decision 2010/87 must be examined by reference to the provisions of the GDPR.").

128. *See* Rustad & Koenig, *supra* note 98, at 376.

129. *See* Tom Brookes, Renée Green & Clive Wong, *Territorial Scope of the GDPR*

No U.S. federal law or statute confers the same broad range of rights as the GDPR, nor does the Constitution enshrine fundamental rights to privacy, like the Charter.[130] Therefore, the U.S. depended on a transatlantic agreement like Privacy Shield to secure a legal pathway for U.S. companies to exchange data with the EU.[131] While 5,000 companies relied upon the former framework — including tech giants like Google, Microsoft, Amazon, Twitter, and Facebook — the end of Privacy Shield shed light on "a fundamental divide between the two economies."[132] First, the CJEU held that U.S. laws did not meet the either the necessity or proportionality requirements according to the GDPR and the Charter. Second, the CJEU ruled that EU subjects whose personal data had been transferred to the U.S. under Privacy Shield, but was later accessed by the NSA, did not have a right to independent and binding redress in U.S. courts.

While the CJEU expressed its disagreements with U.S. privacy law, the court did not specify enforcement mechanisms for nations with inferior privacy rights, like Russia.[133] Moreover, the United States is not utterly devoid of privacy concerns in technology: the Court in *Carpenter* reasoned that technology advancement brings users's data rights closer to the sphere of constitutional protection.[134] Sensitive to this possibility, the Supreme Court did not expand the third-party doctrine in *Carpenter*.[135] Instead, it held that cell-site location, like a person's movements, is a Fourth Amendment privacy interest whose automated collection and analysis is unconstitutional

---

- *Where Does the Boundary Lie?*, ASHURST (Mar. 4, 2020).

130. Silverstein, *supra* note 38, at 215. *But see* The Charter, *supra* note 31.

131. *See* William Alan Reinsch & Isabella Frymoyer, *Transatlantic Data Flows: Permanently Broken or Temporarily Fractured?*, CTR. FOR STRATEGIC & INT'L STUD. (Aug. 31, 2020), https://www.csis.org/analysis/transatlantic-data-flows-permanently-broken-or-temporarily-fractured.

132. *See id*.

133. Marcin Kryszko & Eldar Mansurov, *Russia: Personal Data Transfers to Russia in Post-Schrems II Era*, CEE LEGAL MATTERS (Sept. 7, 2021), https://ceelegalmatters.com/magazine-articles/7568-issue-8-6/17785-russia-personal-data-transfers-to-russia-in-post-schrems-ii-era ("The problem is that with respect to countries like Russia, in most instances there may be no effective and reasonable safeguard. After all, what could two private companies effectively do to prevent Russian authorities from intercepting data? Accordingly, one year after *Schrems II*, almost all personal data transfers to Russia remain in the risk zone . . . [and] termination of all transfers to Russia is not an option.").

134. *See* Carpenter v. United States, 585 U.S. 296, 320 (2018) (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928)) (stating that "the Court is obligated — as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government' — to ensure that the 'progress of science' does not erode Fourth Amendment protections").

135. *See id*.

without a warrant.[136] By doing so, the Court said it was confronting "new concerns wrought by digital technology."[137]

The search for equivalency standards between personal data rights in U.S. and EU law should, therefore, turn to the reasoning in *Carpenter*.[138] This holding favored privacy for the first time in decades, specifically drawing upon its precedent to question the adequacy of the third-party doctrine in the digital age.[139] As a jurisprudential matter, *Carpenter* enhances privacy rights by applying constitutional protections to persons' data in third-party hands.[140] On one level, the Supreme Court was disturbed by the involuntary collection of data through automated means, and also, it considered the weight of individuals' Fourth Amendment privacy interest when it left user's hands.[141] These factors resemble Article 22 of the GDPR: "The data subject shall have the right not to be subject to a decision based solely on automated processing . . . which produces legal effects concerning him or her or similarly significantly affects him or her."[142] point of mutuality regarding inquiry into automated data extraction services extends to industries such as healthcare, finance, and technology.[143]

136. *See id*. at 296–98, 306–07, 313–15.

137. *See id*. at 318–19.

138. Bahar et al., *supra* note 9 ("The upcoming months may prove to be a watershed year for the third-party doctrine, and for the larger debate between the appropriate balance between privacy and security [because] [w]hat is decided in the United States will also have impacts beyond its borders, especially where personal data belonging to non-U.S. residents are being processed by U.S. businesses or within the United States, and could give rise to judicial and legislative conflicts between the United States and Europe.")

139. *See Carpenter*, 585 U.S. at 309–12.

140. *Id*. at 2220; *see also* Marc Rotenberg, *Carpenter Fails to Cabin Katz as Miller Grinds to a Halt: Digital Privacy and the Roberts Court*, AM. CONST. SOC'Y, https://www.acslaw.org/ANALYSIS/ACS-SUPREME-COURT-REVIEW/CARPENTER-FAILS-TO-CABIN-KATZ-AS-MILLER-GRINDS-TO-A-HALT-DIGITAL-PRIVACY-AND-THE-ROBERTS-COURT/ (last visited Jun. 10, 2024) ("Eventually, the Court of Justice of the European Union took up the matter [of data-retention] and concluded that the retention of phone records, of the type at issue in the *Carpenter case*, was a violation of fundamental rights").

141. *See Carpenter*, 585 U.S. at 320 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection").

142. GDPR, *supra* note 15, at art. 22 (Automated Individual Decision-making).

143. Neha Gunnoo, *What is data extraction in 2023? Techniques and Best Data Extraction Tools*, PARSEUR (Feb. 15, 2023) https://parseur.com/blog/what-is-data-extraction (explaining different methods of data extraction used by companies).

Second, concerning cell site location information the Court recognized that the use of a cell phone (to check calls, texts, e-mails, the news, weather, and social media) generates countless data points that a phone automatically links to a user's location.[144] Similarly, EU law codifies rules on connection points and enforces a user's privacy rights during interactions "based solely on automated means," which occur whenever "decisions are taken about [a person] by technological means and without any human involvement."[145] For example, even innocuous services like the flashlight function on a cell phone collect users' location data.[146]

Third, citing the *Olmstead* opinion, the *Carpenter* Court acknowledged that the "makers of [the] Constitution" conferred to citizens the "right to be left alone."[147] Although not equal to the GDPR's affirmative right to erasure (or the right to be forgotten) — where an individual can request that a company delete all the data it has on that individual — the reasoning in *Olmstead* is similar because the text places the Constitution in a protective role when an individual faces an invasion of privacy.[148]

Despite a new analysis of the third-party doctrine in *Carpenter*, the barrier to equivalent standards in privacy law is ultimately a difference of perspective. Whereas the EU law allows users the right to possess or relinquish privacy in certain contexts, U.S. law treats privacy as an indivisible concept, entirely relinquished when turned over to third-party companies.[149] Ironically, corporate entities are able to treat privacy like divisible tokens by collecting and sending data off for monetary value.[150] The third-party doctrine separates users from privacy protections in a society

144. *See Carpenter*, 585 U.S. at 315–16.

145. *See* European Commission, *Can I be subject to automated individual decision-making, including profiling?*, https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_en (last visited Jun. 10, 2024).

146. *See* Wailin Wong & Darian Woods, *The Hidden Market for Your Location Data*, NPR (Nov. 1, 2022) https://www.npr.org/2022/11/01/1133397471/the-hidden-market-for-your-location-data ("It is a multibillion-dollar industry where information on people's precise whereabouts is still being collected from mobile apps and sold to companies or government agencies, often without users' knowledge or direct consent.").

147. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928).

148. GDPR, *supra* note 15, at art. 17 (Right to erasure ('right to be forgotten')); *see also* Michael German, *Restoring the Right to Be Left Alone: Unfinished Business*, BRENNAN CTR. FOR JUST. (Jan. 11, 2016) https://www.brennancenter.org/our-work/analysis-opinion/restoring-right-be-left-alone-unfinished-business.

149. *See* Lawrence Lessig, *Privacy as Property*, 69 SOC. RES. 247, 261 (2002) (arguing that people could have more ownership of privacy if it were treated as property).

150. *See* Valentino-DeVries et al., *supra* note 78.

that exists with the "help of technology, [which] companies [use] today [to] sweep up huge amounts of customer data."[151]

Meanwhile, the GDPR sets rules that consider the divisibility of data, regardless of whether it is shared with third-parties.[152] Compare to the Supreme Court, which cabined its protections by labeling its Carpenter ruling as "a narrow one," and deciding "not [to] express a view on matters not before [the Court]" nor "disturb[ing] the application of *Smith* and *Miller* [by] call[ing] into question conventional surveillance techniques and tools, such as security cameras."[153] Thus, third-party doctrine cases will be determined on a case-by-case basis.[154] When it comes to similarities to the GDPR and the Charter, which imparts the right to privacy to all current and future technologies capable of possessing users' data, *Carpenter* falls significantly short.[155]

Before the rise of digital technology, the dissent in *Smith* predicted that "assuming individuals 'typically know' that a phone company monitors calls" they must forgo "what for many has become a personal or professional necessity, [or else] accept the risk of surveillance."[156] With the nature of modern life, it is hard to conceive that anyone is in exclusive and sole possession of their data given the information-sharing landscape of personal and professional life.[157] Ultimately, the inevitable use of real-world tools abrogate one's privacy under the third-party doctrine.

---

151. *See* Timothy Morey, Theodore Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015) https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

152. *The Quick and Easy Guide for GDPR– Part 3– GDPR in a Nutshell*, COURSEDOT (Mar. 15, 2018) https://coursedot.com/blog/2018/03/19/the-quick-and-easy-guide-for-gdpr-part-3-gdpr-in-a-nutshell/ (stating that the GDPR turns privacy into a property right by enumerating several individual rights for the self-ownership of data: the right to be forgotten, right to object, right to rectification, right to portability, right to access, and right to be notified).

153. *See* Carpenter v. United States, 585 U.S. 296, 315 (2018).

154. *See, e.g.*, United States v. Morel, 922 F.3d 1, 8–9 (1st Cir. 2019) (refusing to expand *Carpenter* to IP addresses); Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 526–27 (7th Cir. 2018) (reasoning that the third-party doctrine is inapplicable to "smart meter" energy data).

155. Julia Powles, *The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy*, NEW YORKER (May 25, 2018), https://www.newyorker.com/tech/annals-of-technology/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy ("[T]he first, ostensibly, is universality: a common set of rules and practices that apply across the Continent and, it is hoped, the world.").

156. *See Carpenter*, 585 U.S. at 336 (J. Marshall, dissenting).

157. *See generally Schrems II*, *supra* note 114.

B. The Impact of Schrems II and Executive Order 14086 on the Transfers of Personal Data

The phrase "third party" appeared exactly once in the Court of Justice for the European Union's judgment invalidating Privacy Shield.[158] The single reference to third-parties expressly proscribes that companies cannot interfere with the fundamental right of privacy.[159] The *Schrems II* court reasoned "that the communication of personal data to a *third party* . . . constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated."[160] Accordingly, to the question of whether the U.S. provides adequate protections for EU data rights, the CJEU answered that it still "harbors doubts" that the potential cross-Atlantic framework will satisfy "Article 45 of the GDPR . . . [and] Articles 7, 8 and 47 of the Charter."[161]

But the judgment also notes that the Charter's fundamental rights do not exist in a vacuum.[162] Rather, the CJEU acknowledged that it should interpret privacy rights with reference to the respective laws of each country – including justiciable limits to the Charter's enumerated rights.[163]

First, the CJEU looked at adjudication by the Foreign Intelligence Surveillance Court ("FISC").[164] Established by Congress through the Foreign Intelligence Surveillance Act of 1978,[165] the FISC has jurisdiction to review, hear, and grant applications for surveillance practices adopted by the U.S. intelligence community.[166] FISA "does not require probable cause or an Article III court-issued warrant because the Fourth Amendment does

158. *Schrems II*, *supra* note 114, at para. 168.

159. *See id*.

160. *Id*. at para. 171 (emphasis in original).

161. *Id.* at para. 168.

162. *See id.* at para. 172 ("However, the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society . . .").

163. *See id.* at para. 174 ("Furthermore, in accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised [sic] by the Charter must be provided for by law and respect the essence of those rights and freedoms . . . limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised [sic] by the Union or the need to protect the rights and freedoms of others.").

164. *Id.* at paras. 179–80.

165. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 103(a), 92 Stat. 1783, 1788 (1978).

166. *Id*. § 1803.

not apply to foreign targets."[167] However, the statute authorized the FISC to conduct a judicial review of the government's collection of foreign intelligence data and demand individualized warrants where necessary.[168]

The CJEU took stock of FISA and the FISC and found that EU subjects lacked "judicial redress possibilities . . . [because the] principle do[es] [not] exist for non-U.S. persons."[169] The court also suspected that "even where judicial redress possibilities in principle [ ] exist for non-U.S. persons, such as for surveillance under FISA,"[170] claims would be inadmissible for lack of standing.

Moreover, cases implicating EU users' data would certainly be read within the a jurisprudence that embraces the third-party doctrine's principles, which is antithetical to Articles 7 and 8 of the Charter.[171] The FISC has no given remedial judgment to third-party doctrine challenges despite the Carpenter ruling. In a declassified opinion, the FISC held that *Smith v. Maryland* "remains controlling" when the government acquired "non-content" telephonic metadata using a third-party provider.[172] According to the FISC, the NSA was allowed to rely on the third-party doctrine as an exception to a warrant requirement when law enforcement accessed the telephone records.[173] The ruling emerged despite evidence of mass surveillance in the United States and abroad.[174] Therefore, it appears likely that legal arguments

---

167. Laila Abdelaziz, *The Ninth Circuit Refuses to Extend the Third-Party Doctrine to NSA Mass Surveillance Program*, AM. U. BUS. L. REV. BUZZ BLOG (Sept. 2020), https://aublr.org/2020/09/the-ninth-circuit-refuses-to-extend-the-third-party-doctrine-to-nsa-mass-surveillance-program/.

168. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 704, 122 Stat. 2436, 2453 (2008).

169. *See Schrems II, supra* note 114, at para. 115.

170. *Id*.

171. *See id.* at para. 171.

172. *See In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], No. BR 13-158, 5 (FISA Ct. Oct. 11, 2013) [hereinafter *In re* Application]; *see also* Cyrus Farivar, *Secret Court Declassifies Opinion Providing Rationale for Metadata Sharing*, ARS TECHNICA (Sept. 17, 2013, 6:00 PM), https://arstechnica.com/tech-policy/2013/09/secret-court-declassifies-opinion-providing-rationale-for-metadata-sharing/ ("Judge Eagan wrote that because terrorists use phones [] and some of those phones traverse the United States' phone network, metadata is therefore considered the business records of the telecoms involved.").

173. *See In re* Application, *supra* note 172, at 5 ("[The] Supreme Court may someday revisit the third-party disclosure principle in the context of twenty-first century communications technology . . . [but] *Smith* remains controlling with respect to the acquisition by the government from service providers of non-content telephony metadata.").

174. *See* Glenn Greenwald*, NSA Collecting Phone Records of Millions of Verizon*

to limit third-party access to digitally-collected information would not pass muster under the FISA-made FISC.[175]

Next, the CJEU also assessed the wide array of bulk collection practices in the U.S. intelligence community.[176] The court criticized the lack of independent oversight[177] and use of bulk collection under Presidential Policy Direction 28 ("PPD-28").[178] Following popular criticism, bulk collection was terminated under FISA and Section 205 of the Patriot Act.[179] Nevertheless, both PPD-28 and the recent Executive Order 14028 have both retained bulk collection programs for signals intelligence.[180]

Many posited that, after *Carpenter*, the third-party doctrine would not extend to bulk collection programs.[181] The former Executive Director of the Privacy and Civil Liberties Oversight Board ("PCLOB") explained that the Supreme Court's decision under *Carpenter* suggested that the "Fourth Amendment [would not] permit[] the bulk collection of telephone records or other digital records" because the Supreme Court's ruling rebuked effortless, encyclopedic compilations of personal data, similar to the aggregate records acquired in bulk collection.[182]

Customers Daily, THE GUARDIAN (June 5, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

175. *See id*.

176. *Schrems II, supra* note 114, at § 43 ("[T]he U.S. government . . . provided the Commission with detailed representations and commitments . . . to create a new oversight mechanism for national security[.]").

177. *Id*. at §§ 183–85 ("It should be added that PPD 28 . . . allows for '"bulk" collection . . . of a relatively large volume of signals intelligence information . . . [but t]hat possibility . . . [is] not circumscribed in a way that satisfies requirements that are essentially equivalent to those required[] under EU law . . .").

178. OFF. OF THE DIR. OF NAT'L INTELLIGENCE, ES 2014-00870, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE PRESIDENTIAL POLICY DIRECTIVE 28 POLICIES AND PROCEDURES 1 (2014) [hereinafter PPD-28] (setting forth the policies and procedures for collection of foreign signals).

179. Charlie Savage, *Obama to Call for End to N.S.A.'s Bulk Data Collection*, N.Y. TIMES (Mar. 24, 2014), https://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html.

180. Exec. Order No. 14086 § 2(c)(ii), 87 Fed. Reg. 62,283, 62,286 (Oct. 14, 2022).

181. *See* Bahar et al., *supra* note 9 ("A decision in the *Carpenter* case could certainly impact the [bulk collection of metadata.]"); *see also* Sharon Bradford Franklin, *Carpenter and the End of Bulk Surveillance of Americans*, LAWFARE (July 25, 2018, 11:36 AM), https://www.lawfaremedia.org/article/carpenter-and-end-bulk-surveillance-americans ("[T]he Carpenter decision should foreclose, once and for all, any claim that bulk surveillance of Americans—or bulk collection of their digital records—would be constitutional.").

182. *See* Bradford Franklin, *supra* note 181 ("[B]ulk telephone records hold the privacies of life in a different, and arguably even more revealing, way [when compared

In reality, *Carpenter* has done little to move intelligence programs away from third-party doctrine bulk collection. Based on a recently unclassified 2020 report on the USA Freedom Act, the PCLOB affirmed the legality of bulk collection despite *Carpenter*.[183] In fact, the PCLOB re-affirmed its previous conclusions from nearly a decade ago – bulk collection of "call detail records" (CDRs) is constitutional under the Fourth Amendment per the third-party doctrine – regardless of new jurisprudence under *Carpenter*.[184]

Given that Executive Order 14086 retains bulk collection, it is possible that the new executive order will face the same pitfalls of EU-U.S. Privacy Shield. First, Executive Order 14086's creation of an independent Data Protection Review Court ("DPRC") to field privacy complaints is no indication that such a court will cabin *Smith* and favor *Carpenter* when it comes to acquiring signals intelligence from third parties.[185] Based on precedent from the Executive Branch,[186] the FISC,[187] and the DPRC's guiding principles of law,[188] the third-party doctrine's stable place in U.S. jurisprudence means that there are no "sufficiently clear and precise limits . . . to delimit the scope of [continued] bulk collection."[189]

---

to the facts in *Carpenter*] . . . [and u]nder *Carpenter*, the third-party doctrine does not extend to the type of collection conducted under the former Section 215 program, and that program would violate the Fourth Amendment.") (internal quotations omitted).

183. PRIV. AND CIV. LIBERTIES OVERSIGHT BD., REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAMS UNDER THE USA FREEDOM ACT 36 (2020) ("Th[e] holding [in *Smith*] remains good law, even as the Supreme Court has clarified the Fourth Amendment's application to new technologies, including cellular networks[.]").

184. *Id*. at 72 ("In [*Smith*], the Supreme Court held that law enforcement collection of certain types of call records is not a 'search' under the Fourth Amendment. The USA FREEDOM Act CDR program involved the collection of call records. Ipso facto, the CDR program is not a search or seizure under the Fourth Amendment.").

185. *See* Exec. Order No. 14086 § 3(d).

186. *See* EUR. PARL. COMM. ON CIV. LIBERTIES, JUST. AND HOME AFF., ON THE ADEQUACY OF THE PROTECTION AFFORDED BY THE EU-US DATA PRIVACY FRAMEWORK 1, 5 (2023) [hereinafter Motion for Resolution] (discussing that the "DCRP is part of the executive branch and not the judiciary" and "can be amended at any time by the US President").

187. *See In re* Application, *supra* note 172, at 2.

188. *See* 28 C.F.R § 201.10 (2022) ("In a DPRC panel's review of an application[,] the DPRC panel shall be guided by relevant decisions of the United States Supreme Court in the same way as are courts established under Article III of the United States Constitution.").

189. *See* EUR. DATA PROTECTION BD., OPINION 5/2023 ON THE EUROPEAN COMMISSION DRAFT IMPLEMENTING DECISION ON THE ADEQUATE PROTECTION OF PERSONAL DATA UNDER THE EU-US DATA PRIVACY FRAMEWORK 134 (2023).

Second, Executive Order 14086 does not prohibit the bulk collection of signals intelligence.[190] The PCLOB concluded that bulk collection is constitutional despite the holding in *Carpenter*.[191] Accordingly, there is no law on point that stops major tech companies from acquiring consumer data in bulk or law enforcement from accessing collected data without a warrant.[192]

Ultimately, the data analytics market accounted for $41.39 billion in 2022 and is projected to grow to $346.33 billion by 2030.[193] For web and technology companies, it is clear that captivating data via individualized experiences – such as online shopping, social media use, search engine innovations, and mobile app development – generates better marketing strategies and attempts to improve consumer experience.[194] Many businesses are building on methods that better reflect users, from their personalities and to complex profiles.[195] Personal data is of interest to entities like data brokers, commercial marketers, and health and financial service providers because it offers a very rich sense of consumer behavior.[196] However, in the absence of law on the point, unregulated markets have been able to build copious data houses that have become the target of ransomware, cybersecurity attacks, and other threats. Current U.S. lawmakers and courts will have to work with, and not around, the competing elements of privacy

190. *See* Motion for Resolution, *supra* note 186, at 5 ("[The] EO [14028] does not prohibit the bulk collection of data by signals intelligence, including the content of communications.").

191. PRIV. AND CIV. LIBERTIES OVERSIGHT BD., *supra* note 183, at 72.

192. *See* Motion for Resolution, *supra* note 186, at 5 ("[The EU Parliament] points out that the EO does not apply to data accessed by public authorities via other means [such as] by commercial data purchases[] or [] voluntary data sharing agreements."); *see also* Kaveh Waddell and Nat'l J*., The NSA's Bulk Collection Is Over, but Google and Facebook Are Still in the Data Business,* THE ATLANTIC (June 3, 2015), https://www.theatlantic.com/politics/archive/2015/06/the-nsas-bulk-collection-is-over-but-google-and-facebook-are-still-in-the-data-business/458496/.

193. PRECEDENCE RSCH., *Data Analytics Market Size to Worth Around USD 346.33bn by 2030*, GLOBENEWSWIRE (Nov. 17, 2022, 10:00 AM), https://www.globenewswire.com/en/news-release/2022/11/17/2558391/0/en/Data-Analytics-Market-Size-to-Worth-Around-USD-346-33-Bn-by-2030.html.

194. *Id.*

195. David C. Edelman & Mark Abraham, *Customer Experience in the Age of AI*, HARV. BUS. REV. (Apr. 2022), https://hbr.org/2022/03/customer-experience-in-the-age-of-ai.

196. Alex Hern, *Amazon Web Services: The Secret to the Online Retailer's Future Success*, GUARDIAN (Feb. 2, 2017, 2:00 PM), https://www.theguardian.com/technology/2017/feb/02/amazon-web-services-the-secret-to-the-online-retailers-future-success.

and security.[197] The unequivocal line drawn in *Smith* is untenable within the current interconnected and increasingly digitized world.[198] It is possible for the U.S. to form law that overcomes the analog-era barrier of the third-party doctrine, otherwise, the lack of change has the ability to forestall seamless data transfers across the Atlantic.[199]

IV. THE SUPPLY OF TRANS-ATLANTIC DATA AND THE DEMAND FOR MODERN PRIVACY LEGISLATION

> Individuals have become "*dividuals*" . . . . [M]an is no longer man enclosed but man in debt.[200]

A. Federal Privacy Legislation Modeled After the GDPR

Constitutional interpretation is not the only means available to effect change. Given the ongoing evolution of technology, U.S. lawmakers are uniquely situated to create federal law that protects consumer data in the digital era. Therefore, the EU's GDPR should serve as a proximate example of how to protect consumer data in the digital world.

As the U.S. economy becomes increasingly digitized, federal law can model several GDPR protections to safeguard online privacy. Legislative measures could enforce company transparency on data usage, mandate notice requirement for data breaches, create a uniform statement on privacy, require explicit consumer consent for retention and use, and give consumers the right to access and amend collected data.

The GDPR provides overarching, mandatory, and centralized guidelines that businesses can readily follow. The alternatives, from frequently changing privacy guidelines to decentralized state models, result in inconsistent and unreliable rules. Adopting legislation similar to the GDPR would ensure that all U.S. companies uphold the same high standards of data rights, regardless of location. Legislation would help the U.S. remain competitive in the global digital economy. After all, users already benefit by providing companies with personal data in exchange for convenience. For example, companies adopt services from user data: faster checkouts, automated shipping, tailored online experiences, and seamless purchases. Technological advancements have generated not only convenience but also empowered individuals to communicate with friends and family from across

197. *See generally* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO L.J. 115 (2017).

198. *See id*.

199. *See id*.

200. Gilles Deleuze, *Postscript on the Societies of Control*, 59 MIT PRESS 3, 5–6 (1992).

the globe, shop for goods or services from the comfort of home, learn new skills and languages, and other feats once unimaginable.

Within a GDPR framework, users would control their contributions of personal data to the market with the expectation of an improved user experience. More users may be willing to provide companies with personal data if they understand the scope of data regulation. For instance, education on different disciplines online, which has generally democratized knowledge, is correlated with the rise of the internet. Ultimately, the data exchange between people and online companies can be framed as a power struggle, with each actor vying for control of their electronic environment. However, by offering users greater rights to their data, people can directly influence the technological products they use, thus creating a sense of overall online control. That response would counter the disempowering user experience with technology today.

The third-party doctrine undermines both users' feelings of control and their trust in technology because data can be sanctioned off to government monitoring anytime it is shared with an internet service provider, cloud service, mobile phone company, or social media platform. Emerging from a distrust in government, the Edward Snowden leak jeopardized U.S. security interest worldwide. Ironically, congressional action against TikTok for its connection to the government of China was based on similar fears: freely accessible data by a government. It would be disingenuous to ignore these public sentiments about data privacy when the purported surveillance occurs domestically. The GDPR framework can empower user decision-making, increase literacy in technology, enhance data sharing, and ease data transfers with mutual partners.

Adopting similar legislation in the United States would enhance trust as the next generation of users come of age. Because technology is essential for any nation that wishes to remain competitive in the global data marketplace, legislation like the GDPR would address modern anxiety surrounding online data and boost trust in the digital economy.

B. A Modern Factors Analysis

It is no secret that criminal actors and adversarial foreign governments can exploit digital technologies for malicious ends. But rapid technological security ambitions have often run against privacy concerns. Accordingly, U.S. law should begin to balance these factors: the government's legitimate requests to obtain information from third parties and individual's privacy interests at stake. A modern factors analysis would convene concerns about the government's degree of intrusion. It would fill in gaps that third-party doctrine's categorical approach to technology. It would bring oversight over compelling private information without a warrant.

Security and privacy are both necessary elements of U.S. democracy: the right to privacy can be protected, and at the same time, surveillance programs can protect civil liberties from criminal actors that wish to cause individual's harm. A balancing test could consider five elements:

First, the nature and sensitivity of the personal information at issue: the more sensitive the personal information, the greater the privacy interest at stake, and the more weight should be given to protecting that information.

Second, the extent to which the individual has voluntarily disclosed the information to a third party: if the individual has voluntarily disclosed the information to a third party, such as by using a social media platform or by providing personal information to a company in order to purchase goods or services, the third-party doctrine may weigh more heavily.

Third, the extent to which the individual has taken steps to protect their privacy: if the individual has used privacy settings or encryption, this may weigh in favor of greater privacy protection.

Fourth, the purpose for which the government is seeking the data: if the government seeks data for a national or public security reason, this may weigh in favor of the third-party doctrine.

Fifth, the extent to which the government could obtain the information through other means: if the government has less intrusive means available, such as through an appropriate warrant or by accessing public records, this may weigh in favor of protecting privacy rights.

Like other factors analyses, courts could analyze a case in its totality and decide if the intrusion on the individual's privacy is outweighed by the particular needs of the government or law enforcement. A factors analysis would invite nuance to modern life, where privacy rights of individuals and important security risks of the government are weighed together.

V. CONCLUSION

The third-party doctrine is a blunt tool. When daily life revolves alongside third-party technology, the vision of privacy set forth by the doctrine is not viable. As jurisprudence for privacy law in the digital age, it has pushed Europe and the United States apart. In the digital marketplace, conflicting data privacy obligations expose U.S. companies like Google, Meta, Amazon, and Microsoft, which abide by both U.S. and European law, to regulatory actions, substantial fines, and injunctions. Considering the foregoing, the U.S. may be left behind in a data-centered world where users expect more protection.