DIGNITY, FREEDOM, AND DIGITAL RIGHTS: COMPARING AMERICAN AND EUROPEAN APPROACHES TO PRIVACY

Virginia Kozemczak[†]

TABLE OF CONTENTS

I. INTRODUCTION

In April of 2019, *The New York Times* announced its new "Privacy Project," a monthlong series of editorials, reports, and commentaries that convened a debate over the state of digital privacy.[1] As written by the Editorial Board, the scope of privacy rights is a hotly debated topic: "[t]he boundaries of privacy are in dispute, and its future is in doubt."[2] The Privacy Project dedicated itself to asking

† Policy Counsel, International Digital Accountability Council*; J.D. Graduate, Benjamin N. Cardozo School of Law, 2020. I would like to thank Professor Burstein for serving as an invaluable advisor and mentor throughout the writing process. I am especially grateful to my husband, Eli, and my entire family for their encouragement and support. *The views expressed in this Note are my own and do not reflect those of the organization.

1 The Editorial Board, *The Privacy Project*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html.

2 *Id*.

whether we as a society are "making the wisest tradeoffs"[3] between the benefits and drawbacks of citizens' diminishing privacy. In a related editorial, James Bennet noted how public anxiety about privacy is growing because "technology has transformed the real and virtual worlds."[4] As such, the public seems particularly troubled by the fact that laws are failing to sufficiently protect them against the pervasive practice of data collection by private companies and governments.[5]

Privacy is widely accepted as fundamental to a healthy, robust society, and most liberal democracies have at least some laws or regulations that protect it.[6] Privacy is also an incredibly multi-faceted concept that has evolved over time.[7] The rapid acceleration of technology continually challenges our sense of what should be considered private.[8] Mobile and portable technologies and the Internet-of-things have enabled a handful of companies to record and track more data about their users in unprecedented ways. Today, our cell phones, portable laptops, and smart devices store and exchange our most intimate information, including our financial data, private messages, and pictures of family and friends.[9]

---

3 *Id.*

4 James Bennet, *Do You Know What You've Given Up?*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/2019/04/10/opinion/privacy-project-launch.html.

5 DANIEL SOLOVE, UNDERSTANDING PRIVACY 2 (2010) [hereinafter SOLOVE] ("Widespread discontent over conceptualizing privacy persists even though privacy is an essential issue for freedom and democracy.").

6 Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 CONN. J. INT'L L. 257, 261 (2013). *See also* SOLOVE, *supra* note 5, at 2 ("Privacy is an issue of profound importance around the world. In nearly every nation, numerous statutes, constitutional rights, and judicial decisions seek to protect privacy.").

7 *See generally* James*, supra* note 6.

8 SOLOVE, *supra* note 5, at 4 ("Since antiquity, people in nearly all societies have debated issues of privacy, ranging from gossip to eavesdropping to surveillance. The development of new technologies kept concern about privacy smoldering for centuries, but the profound proliferation of new information technologies during the twentieth century—especially the rise of the computer—made privacy erupt into a frontline issue around the world.").

9 *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights,* AMNESTY INTERNATIONAL (2019) https://www.amnesty.at/media/6430/amnesty-surveillance-giants_bericht-november-2019.pdf . ("Over half of the world's population now relies on the web to read the news, message a loved one, find a job, or seek answers to an urgent question. . . These [] companies collect extensive data on what we search; where we go; who we talk to; what we say; what we read; and, through the analysis made possible by computing advances, have the power to infer what our moods, ethnicities, sexual orientation, political opinions, and vulnerabilities may be.").

While privacy is a widely shared value, its historical roots and legal manifestations vary greatly.[10] The United States and the European Union, in particular, have experienced a "transatlantic clash" over privacy rights.[11] Whether regarding the "right to be forgotten"[12] or the EU-U.S. Privacy Shield,[13] which governs how companies transfer data from the EU to the United States,[14] American and European citizens tend to have very different expectations of privacy.[15] This difference is important because the U.S. and Europe, are major players in shaping privacy norms, as they house the world's major tech companies.[16] And although the U.S. and Europe share a similar "intuition" that privacy is indispensable, society is nonetheless "shaped by the prevailing legal and social values of the societies in which we live."[17] Therefore, this Note examines the differences between the U.S. and EU's prevailing legal and social values to identify how and why privacy laws are struggling to adequately protect us.

In the U.S., laws protecting personal data consist of "a patchwork quilt" comprised of common law, state and federal statutes, regulations, and the U.S. Constitution.[18] In the age of rapid technological change, this "piecemeal approach [is] increasingly problematic"[19] resulting in a "reactive, adaptive process [] by the courts."[20] As such, the U.S. Supreme Court has failed to articulate a

---

10 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE. L.J. 1151, 1160–61 (2004).

11 *Id.* at 1153.

12 Steven C. Bennett, *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 164-66 (2012) (discussing American criticisms of Europe's embrace of the right to be forgotten).

13 Mark Scott, *U.S. and Europe in "Safe Harbor" Data Deal, but Legal Fight May Await*, N.Y. TIMES (Feb. 2, 2016), https://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html.

14 *Id*.

15 Whitman, *supra* note 10, at 1153–60.

16 John McKenna, *Europe's tech giants are growing. These are some of the biggest,* WORLD ECONOMIC FORUM (Oct. 6, 2017), https://www.weforum.org/agenda/2017/10/meet-europe-top-tech-titans/.

17 *Id.* at 1160.

18 Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OF OTTAWA L. & TECH. J. 357, 360 (2005).

19 *Id.* at 361.

20 *Id.* at 361-62.

theory of privacy that is consistent and comprehensive.[21] Critics have gone so far as to say that the law is simply not keeping with this age of technology.[22]

This Note considers the ways in which courts in the United States and European Union have interpreted the Fourth Amendment of the U.S. Constitution and Article 8 of the European Convention on Human Rights, respectively. In particular, it focuses on the ways in which the Fourth Amendment and Article 8 have functioned as legal tools protecting individuals' privacy against government intrusion. Here, I specifically examine cases regarding state surveillance that have utilized cellphone geolocation data and Internet Protocol ("IP") addresses which all raise difficult questions around citizens' ability to opt-out of data collection and what precisely constitutes personal information. The U.S. and the EU's contrasting approaches to these types of cases illuminate the distinct conceptions of privacy which they each possess. Ultimately, the Note contends that the U.S. courts are not properly protecting citizens' privacy—even by their own standards—and that adopting a version of Europe's approach would remedy those shortcomings.

First, this Note will provide a brief overview of privacy and how we attempt to define it. Second, it will provide a brief overview of Fourth Amendment jurisprudence and how it has been applied in the digital age, namely in the landmark case of *U.S. v. Carpenter*. Third, this Note looks at the aftermath of *Carpenter* and examines its shortcomings considering these differences. Fourth, this Note will provide a brief overview of the European Convention on Human Rights, specifically Article 8, and explain how it has also been applied within the digital age. The Note concludes with a discussion regarding a comparison of EU and U.S. privacy principles. This comparison is done with the aim of inviting U.S. privacy law to incorporate more European and international legal norms.

II. BACKGROUND

Europe and the United States' distinct social and political traditions contributed to unique perceptions of privacy, which are

---

21 Daniel J. Solove*, Fourth Amendment Pragmatism,* 51 B.C. L. REV. 1511, 1512 (2010) (discussing that "most commentators have recognized that . . . Fourth Amendment doctrine is in a state of theoretical chaos.").

22 *See, e.g.*, Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 71 (2005) (criticizing the U.S. Supreme Court's approach to privacy as inadequate to deal with new technology).

reflected in the European and American legal systems.[23] On the one hand, Europeans see privacy as an aspect of personal dignity.[24] The sacredness of dignity in the privacy context is enshrined in the European Charter of Fundamental Rights and the European Convention on Human Rights, which are examined in greater detail in Section V. Legal scholar James Whitman claims that dignity has manifested in Europe as a preoccupation with the ability to control one's "image, name, and reputation."[25] Put simply, Europeans strongly believe that people have a right to be seen the way that they want to be seen.[26] Closely related to this ability to control one's image and reputation is the espoused principle of "informational self-determination" or the right to control information about oneself.[27] Informational self-determination is perhaps most embodied in the General Data Protection Regulation ("GDPR"), which in over-simplified terms, gives data subjects the right to see what data has been collected about them and mandates that businesses clearly disclose data collection practices.[28] Whitman believes that control over one's image and informational self-determination are two sides of the same coin: they serve as guarantees that citizens are able to control their public image.[29]

In contrast, the United States has historically prioritized a conception of privacy as liberty.[30] As Whitman points out, Americans hold dearly the individual's "liberty against the state"[31] and "freedom from intrusion . . . especially in [the] home."[32] Nevertheless, although it is true that privacy-rooted-in-dignity is broadly embraced by Europe, and privacy-rooted-in-liberty is broadly embraced by the

---

23 Whitman, *supra* note 10, at 1160.

24 *Id.* at 1160-61.

25 *Id.* at 1161.

26 *Id.*

27 *Id.*

28 Matt Burgess, *What is GDPR? The summary guide to GDPR compliance in the UK*, WIRED MAGAZINE (Jan. 21, 2009), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

29 Whitman, *supra* note 10, at 1161 ("The core continental privacy rights are rights to one's image, name, and reputation, and what Germans call the right to informational self-determination-the right to control the sorts of information disclosed about oneself**.** These are closely linked forms of the same basic right: They are all rights to control your public image-rights to guarantee that people see you the way you want to be seen.").

30 *Id.*

31 *Id.*

32 *Id.*

U.S.,[33] there is certainly an overlap between the two. As Whitman admits, "it would be wrong to say that there is some absolute difference" between European and American privacy. Dignity has appeared throughout American legal jurisprudence,[34] and American legal scholar Samuel D. Warren and eventual Supreme Court Justice Louis D. Brandeis argued for the "right to be let alone" as means to control one's reputation.[35] In their seminal work, *The Right to Privacy*, Brandeis and Warren bemoaned the tabloid press and muckraking journalists of the time, criticizing the "inva[sion] [of] the sacred precincts of private and domestic life."[36] Similarly, European courts have heard many cases regarding an individual's freedom from government intrusion, as examined in Section VI.

Still, even if we understand the historical roots and values of privacy in Europe and America, it leaves open the question of what we mean by "privacy" itself. Privacy is commonly discussed, yet it is surprisingly difficult to define.[37] Daniel Solove writes that privacy is "a concept in disarray,"[38] while Whitman calls it "an unusually slippery concept."[39] Oftentimes, however, the definition of privacy depends upon context and circumstance.[40] It may refer to "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, [or] protection from searches and interrogations."[41] Solove proposes a "taxonomy" of privacy, in which he identifies four types of activities that concern individuals' interests in privacy: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion.[42] For instance, examples of "information collection" include investigators conducting surveillance or a social media site amassing its users' personal data. "Information processing" entails

---

33 *Id.*

34 Leslie Meltzer Henry, *The Jurisprudence of Dignity*, 160 U. PENN L. REV. 169 (2011).

35 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

36 *Id.* at 195 ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life.").

37 SOLOVE, *supra* note 5, at 1; Whitman, *supra* note 10, at 1153; James, *supra* note 6, at 259.

38 SOLOVE, *supra* note 5, at 1.

39 Whitman, *supra* note 10, at 1153.

40 James, *supra* note 6, at 259 ("The term 'privacy' has a multitude of complex meanings and connotations, some of which are dependent on equally complicated cultural norms.").

41 SOLOVE, *supra* note 5, at 1.

42 *Id.* at 10.

activities that aggregate data in invasive ways, such as when websites compile and process behavioral data. "Information dissemination" involves breaches of confidentiality or disclosure of private facts,[43] or perhaps what Whitman would call the loss of the ability to control one's reputation.[44] Lastly, "invasion" refers to intrusions, which may include literal intrusions like wiretapping or videorecording, or more institutional ones, such as those that limit private choices regarding marriage or abortion.[45]

In this Note, I will add a different kind of taxonomy to Solove's and Whitman's. Whitman's categories describe privacy in terms of the values that are rooted in dignity or liberty. Solove's categories, further still, describe the activities whereby privacy concerns are likely to arise: information collection, processing, dissemination, and invasion. Here, I offer categories that attempt to capture the discourse surrounding societal expectations of how privacy laws and regulations should operate. As privacy scholar Ari Waldman points out, "privacy is an inherently social concept"[46] that manifest in our relationships with other parties.[47] When we make decisions regarding how and when we share information, we "rely on and develop expectations about what should happen to our information based on the contexts in which we share. . . ."[48] The key word here is *expectation*, and as such, the definitions I offer below attempt to capture what our societal expectations of privacy laws and regulations are.

For instance, during the Cambridge Analytica scandal, it was revealed that the political data firm gained access to the private information of more than fifty million Facebook users.[49] After users took a personality survey, a smartphone app collected information from their Facebook profiles as well as their friends.[50] Millions of people felt violated after their information was collected and

---

43 *Id*.

44 Whitman, *supra* note 10, at 1161.

45 SOLOVE, *supra* note 5, at 11.

46 ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 3 (2018).

47 *Id.*

48 *Id*.

49 Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

50 *Id*.

processed without their consent.[51] In this instance, Facebook users were appalled at the way that their data was taken, analyzed, and disclosed.[52] Certainly, Cambridge Analytica's actions violated the personal dignity of these users. As evidenced by the subsequent public outrage, users believed they had a right to manage and control how their personal data was being used.[53] Users' sense of justice, of right and wrong, included the belief that some kind of rule or regulation was necessary in order to control their information and online reputations. This concept of privacy is what I will call "privacy-as-*tractatio*." *Tractatio* is a Latin term, meaning the "handling, wielding, management, [or] treatment" of something,[54] and privacy-as-*tractatio* refers to the kind of exchange that occurs when parties entrust some aspects of their private information to others. Persons are willing to entrust a party with some sensitive information but, continue to expect that it will be managed in a fair and just manner. The Cambridge Analytica scandal is just one example in which users' privacy-as-*tractatio* was violated. Although privacy-as-*tractatio* shares similarities with Waltman's privacy-rooted-in-dignity, and Solove's information collection and dissemination, it is not categorically the same.[55] Privacy-as-*tractatio* could involve citizens' relationship with the government and concerns for liberty, for instance. After all, we citizens accept the need for state-sanctioned driver's licenses and body scanners at the airport, so long as the law justly governs the handling

---

51 *See* Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, THE GUARDIAN (Mar. 17, 2018) ("The revelations provoked widespread outrage."). *See also* Iga Kozlowska, *Facebook and Data Privacy in the Age of Cambridge Analytica*, UNIVERSITY OF WASHINGTON, LATEST NEWS (Apr. 30, 2018), https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/. ("[T]he public outcry reveals that [Facebook users] [did] not feel that they authorized the app to access their data. . .").

52 *Id.*

53 Jim Isaak and Mina Hanna, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,* COMPUTER 56, 59 (Aug. 2018) https://ieeexplore.ieee.org/abstract/document/8436400/

54 *An Elementary Latin Dictionary*, PERSEUS DIGITAL LIBRARY, http://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.04.0060:entry=tractatio (last visited Feb. 8, 2021).

55 Government bodies issue driver's licenses and mandate airport security without public outcry because those governance and security measures reflect our social values in those areas. Waldman states that privacy-as-trust "reflects our social values. . .[and] empirical evidence of our social behavior."

and management of that data.[56] Privacy-as-*tractatio* is similar to Waldman's conception of *privacy-as-trust*; Waldman describes trust as a "resource of social capital between or among two or more parties concerning the expectation that others will behave according to accepted norms."[57] Disclosure of information, such as Internet users navigating Facebook, happen "in [the context] of trust, and trust is what's broken when data collection and use go too far."[58] Disclosure by itself is not harmful, Waldman argues; in fact, it is necessary in society and occurs widely, such as between doctors and patients, as well as attorneys and clients.[59] What is crucial, however, is that disclosures "occur in safe environments buttressed by concurrent norms of confidentiality and discretion."[60] And while trust is a key component in these contexts, I nevertheless will use the term "privacy-as-*tractatio*" to capture individuals expectation that they may control, manage, access, and of course, entrust their information with and to, other parties.

On the other hand, privacy may also refer to people's desire for protection against intrusive surveillance. I call this second category "privacy-as-aegis." Aegis refers to "protection," and to the shield that was associated with Zeus and Athena in ancient Greek mythology.[61] In this context, citizens expect privacy laws and regulations to act as a bulwark against bad actors and expect freedom from unlawful surveillance and the ability to control one's own body. Furthermore, privacy-as-aegis and privacy-as-*tractatio* are not mutually exclusive. For instance, if the U.S. government were to weaken tech companies' encryption practices for its criminal investigations, citizens' privacy-as-aegis—their shield against government intrusion—would be weakened.[62] As a result, weaker encryption would put the security of

---

56 *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 72.

57 WALDMAN, *supra* note 41, at 4.

58 *Id.*

59 *Id*.

60 *Id.*

61 *Definition of aegis*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/aegis (last visited Feb. 8, 2021).

62 *See generally* Kian Vesteinsson, *US Government Challenges Apple on Encryption (Again)*, HUMAN RIGHTS WATCH DISPATCHES (Jan. 16, 2020), https://www.hrw.org/news/2020/01/16/us-government-challenges-apple-encryption-again. *See also* Shahid Buttar, *Apple, Americans, and Security vs. FBI*, ELECTRONIC FRONTIER FOUNDATION (Feb. 20, 2016), https://www.eff.org/deeplinks/2016/02/apple-americans-and-security-vs-fbi.

users' iPhone data at a risk.[63] As such, iPhone users' privacy-as-*tractatio* and their ability to manage and control their data on Apple devices—would be compromised.[64] In summary, privacy-as-*tractatio* and privacy-as-aegis are two closely related and overlapping concepts.

These categories are useful because they describe how the law functions, or, in some circumstances, how the law *ought* to function. It speaks to what individuals are *seeking* from their privacy laws. In the forthcoming sections, I will analyze the ways in which these various definitions of privacy are discussed by both American and European courts.[65]

III. PRIVACY RIGHTS IN THE UNITED STATES

According to Louis Fisher and David Adler, privacy is commonly conceived of as a natural right, as "[a]reas of private conduct and thought have always been protected from state intrusion."[66] For instance, the widely influential British philosophers John Locke and John Stuart Mill wrote that freedom from state interference served as a central tenet of liberal democracy.[67] The importance of *freedom from intrusion* influenced American thinkers, including James Madison, the "Father of the Constitution."[68] Madison's writings capture the heart of American privacy, which is "primarily motivated by the protection of liberty"[69] and "American concerns about 'Big Brother' government."[70] To Madison, freedom from unlawful search and seizures was intrinsically connected to property rights: just as individuals have land or materials, they too "ha[ve] property in [their] opinions and the free communication of them."[71] This property interest "in the free use of [] faculties" is "a natural and inalienable right" that cannot be violated without due process.[72] The Bill of Rights was a direct response to the perceived government overreach in

---

63 *Id.*

64 *Id.*

65 Cases discussed in forthcoming sections hail from the Supreme Court of the United States and the European Court of Human Rights.

66 LOUIS FISHER & DAVID GRAY ADLER, AMERICAN CONSTITUTIONAL LAW 891 (7th ed., 2007).

67 James, *supra* note 6, at 261.

68 *Father of the Constitution*, LIBRARY OF CONGRESS, https://www.loc.gov/wiseguide/may05/constitution.html (last visited Feb. 8, 2021).

69 Levin & Nicholson, *supra* note 18, at 360.

70 *Id*.

71 *See* 6 THE WRITINGS OF JAMES MADISON 101-03 (Gaillard Hunt ed., 1906).

72 *Id*.

Britain, including overzealous police activity.[73] The authors of the Constitution remembered how British officials abused their power by conducting searches on citizens.[74] Therefore, the Fourth Amendment of the Constitution protects against wrongful intrusions by the state,[75] assuring that citizens must be "secure in their persons, houses, papers, and effects."[76] Furthermore, in order to search and seize any person or item, the government must obtain a warrant from an independent magistrate judge based on probable cause.[77]

As such, American jurisprudence focused on personal property, particularly the home, when interpreting the Fourth Amendment.[78] As Whitman writes, American anxieties saw intrusion upon "the sanctity of the home" as a real threat.[79] The goal of American privacy law, then, was to ensure that an individual could "[maintain] private sovereignty within [his] own walls."[80] Clearly, the Fourth Amendment not only has its roots in liberty, as suggested by Whitman,[81] but also privacy-as-aegis: as a (figurative) wall that forcefully shuts out "Big Brother" government. Because privacy centered so strongly around private property, the U.S. Supreme Court originally conceived *intrusions* of privacy only as physical intrusions.[82] For instance, in 1928, the Court was faced with the question of whether wiretapping a telephone was covered under the Fourth Amendment in *Olmstead v. United States*.[83] The Court held that it was *not* because "[t]here was no entry of the houses . . . ."[84] However, as technology developed, the

---

73 JOSHUA DRESSLER & GEORGE THOMAS III, CRIMINAL PROCEDURE, PRINCIPLES, POLICIES AND PERSPECTIVES 11-14 (6th ed., 2016) ("With the writs of assistance and excise searches by British officials still fresh in their minds, the Anti-federalists saw potential abuses of federal power everywhere they looked . . . The deep-seated fear of the central government led directly to the drafting and ratification of the Bill of Rights. Early Americans viewed the Bill of Rights as a wall between themselves and the central government.").

74 *Id*.

75 *Id.*

76 U.S. CONST. amend. IV.

77 *Id.*

78 Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

79 Whitman, *supra* note 10, 1162, 1211-12, *citing* Boyd v. United States, 116 U.S. 616, 630 (1886).

80 Whitman, *supra* note 10, at 1162

81 *Id.*

82 DANIEL SOLOVE, THE DIGITAL PERSON 196-97 [hereinafter THE DIGITAL PERSON] ("[T]he Court viewed invasions of privacy as a type of physical incursion.").

83 Olmstead v. United States, 277 U.S. 438, 464–66 (1928).

84 *Id*.

line between private property and the public domain became increasingly blurred.

In *Katz v. United States,*[85] the Supreme Court's ruling marked a pivotal moment in Fourth Amendment jurisprudence.[86] The facts of *Katz* are as follows. Law enforcement suspected that Katz was engaged in illegal activities.[87] While Katz was using a public phone booth, officials attached a device to the booth and listened to Katz's phone call.[88] The government argued that Katz was in public, therefore the Fourth Amendment's warrant requirement did not apply.[89] The Court disagreed and overruled *Olmstead* "[t]he Fourth Amendment protects people, not places."[90] The Court also articulated the "reasonable expectation of privacy test," which currently governs the scope of Fourth Amendment protection.[91] Since the *Katz* decision, the Fourth Amendment has been significantly shaped by the reasonable expectation privacy test. The Court now asks whether a person has an "expectation of privacy" that society recognizes as "reasonable."[92] If the expectation is reasonable, then the government must obtain a warrant based on probable cause.[93] If it is not, then the government's search or seizure is reasonable.[94]

In plainer terms, when a person purchases an item in a store or walks around in public, they clearly understand that their actions are not private, unlike those in their home. Therefore, that individual cannot be said to have an expectation of privacy. In any circumstance—for people driving in their cars, texting in their workplaces, etc.—the Court asks whether that expectation is one that is widely shared with society.[95] On the other hand, the more that someone "assumes the risk" of exposing herself, the less that she

---

85 Katz v. United States, 389 U.S. 347, 353 (1967).

86 Daniel Solove, *Fourth Amendment Pragmatism*, 51 B.C.L. REV. 1151, 1151 (2010) [hereinafter *Fourth Amendment Pragmatism*].

87 *See Katz*, 389 U.S. at 348-350.

88 *Id.*

89 *Id.*

90 *Id.* at 351.

91 *See id.* at 351 ("For the Fourth Amendment protects people, not places."); *see also id.* at 360-61 (Harlan, concurring) ("[A] person has a constitutionally protected reasonable expectation of privacy.").

92 *Katz,* 389 U.S. at 360-61 (Harlan, concurring).

93 *Id.*

94 *Id.*

95 *Id*. at 361. (". . .that the expectation be one that society is prepared to recognize as 'reasonable.'").

should expect privacy, in addition to Fourth Amendment protection.[96] Importantly, the test requires two parts: "first, whether the individual has exhibited an actual (subjective) expectation of privacy; and second, whether his expectation is one that society is prepared to recognize as 'reasonable.'"[97]

A closely related doctrine is the "third-party principle," which states that personal information "used in commercial transactions" such as bank checks "are not confidential communications," but are instead "information voluntarily conveyed . . . in the ordinary course of business."[98] The reasoning goes that because individuals engage with and willingly exchange information with a third-party, such as a bank or other business, they understand that their information is not totally private. Therefore, if law enforcement is to subpoena a third-party and request that information, the Fourth Amendment has not been violated.[99] Similarly, call records, or "pen registers," are also subject to the third-party doctrine[100] because when an individual sets up a phone account with a telephone company and uses its services, she has conveyed this information to the company, "assuming the risk" that it could one day end up in the hands of law enforcement.[101]

Once again, however, technology came along and complicated matters.

IV. FOURTH AMENDMENT PROTECTIONS IN THE DIGITAL AGE

When the Internet emerged, American legal scholars reconceptualized the "reasonable expectation of privacy" test in the digital era. As Orin Kerr notes,[102] some of the earliest cases which emerged during the late 1990s involved Internet Protocol addresses.[103] In most IP address cases:

> "investigators learn that an individual has been using a specific Internet account to distribute or seek images of child pornography . . . Investigators then subpoena the Internet service provider (ISP) associated with that address. . . After

96 Smith v. Maryland, 99 S. Ct. 2577, 2585 (1979).
97 Carpenter v. United States, 138 S. Ct. 2206, 2577 (2018).
98 United States v. Miller, 96 S. Ct. 1619, 1624 (1976).
99 *Id.*
100 *See Smith*, 99 S. Ct. at 2586.
101 *Id.* at 2585.
102 Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1005 (2010) [hereinafter Kerr].
103 *Id.* at 1026.

> a search warrant reveals contraband [], the defendant challenges the collection of his home address."[104]

According to Kerr, courts have "uniformly concluded" that Fourth Amendment protections do not apply to the collection of home addresses using this method.[105]

Kerr theorizes a way to "map on" the reasonable expectation of the privacy test to the Web by making a distinction between *data with content*—such as the content of e-mails, telephone calls, and texts—and *non-content data*—such as the time and place an e-mail, call or text and the e-mail address or phone number receiving the communication.[106] According to Kerr, at its heart, the Fourth Amendment aims to protect our private lives inside our homes, but not our public actions outside those four walls.[107] In digital spaces, Kerr writes, "courts should treat non-content information relating to communications as if it were functionally 'outside' and content information as if it were functionally 'inside'. . . [The reason is] outside surveillance [pertains] to identity, location, and time. . . Inside surveillance more often exposes private thoughts."[108] Kerr appears to epitomize Whitman's American conception of privacy, emphasizing freedom of thought and speech, caring less about the ability to control one's own identity. In the IP address cases, Kerr argues that the Internet Protocol address functions like "outside-the-property" data.[109]

Once again, however, new technology challenged traditional legal conceptions. In 2018, the U.S. Supreme Court decided *Carpenter v. United States*,[110] a significant case in American privacy law. Although the holding in *Carpenter* was narrow, the Court acknowledged that the reasonable expectation of privacy test needed a new examination.[111]

---

104 *Id.*

105 *Id.*

106 *See generally* Brief of Professor Orin S. Kerr as Amicus Curiae, 4-7, Carpenter v. U.S., 138 S. Ct. 2206 (2018) (https://www.scotusblog.com/wp-content/uploads/2017/10/16-402-bsac-Orin-Kerr.pdf). *See also,* Orin. S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 3 MICHIGAN L. REV. 317 (2012) [hereinafter *Mosaic Theory*].

107 Kerr, *supra* note 102, at 1009-11.

108 *Id.* at 1018.

109 *Mosaic Thepry, supra* note 106.

110 Carpenter v. U.S., 138 S. Ct. 2206, 2211-23 (2018).

111 *Id.* at 2214. ("This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents.").

A. A Turning Point: Carpenter v. United States

Before the Supreme Court issued the *Carpenter* opinion, investigators were permitted to obtain cellphone location records ("CSLI") from third party cell phone providers under the Stored Communications Act ("SCA").[112] Historical CSLI records provide remarkably accurate information about the location of an individual's movements.[113] The scope of the record is large, as it may include the individual's location at a given time for weeks or months.[114] The SCA had stipulated that the government may request these kinds of records when "specific and articulable facts show that there are reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation."[115] In other words, investigators were not required to obtain a warrant premised on probable cause, so long as the records sought pertained to an investigation.[116]

To identify and arrest several men connected to a number of armed robberies, law enforcement requested the cell phone records of suspects under the SCA.[117] The CSLI data included the time and date of the calls in addition to where the caller was approximately located.[118] Based on evidence obtained from the surveillance, Timothy Carpenter was charged with several crimes, but argued that the government needed a warrant to request the CSLI records.[119]

Put more simply, the Court agreed that using the CSLI data violated the Fourth Amendment and that the mode of surveillance used to obtain the data was too broad and intrusive.[120] The Court based its opinion on various factors; namely, it did not believe that the third-party doctrine should be applied to CSLI records.[121] The underlying reasoning was, while eye-witnesses may tell investigators the past whereabouts of a suspect, it pales in comparison to the kind of detailed, precise information that CSLI records provide.[122] For instance, this information "painted a detailed picture of [Carpenter's] life" and provided an "exhaustive chronicle of location

---

112 U.S. Const. IV amend.; 18 U.S.C.A. § 2703(d).
113 *See Carpenter*, 138 S. Ct. at 2210.
114 *Id.*
115 18 U.S.C.A. § 2703(d).
116 *See Carpenter*, 138 S. Ct. at 2213.
117 *See id.* at 2211-14.
118 *Id.*
119 *Id.*
120 *Id.*
121 *Id.* at 2240-45.
122 *Id.* at 2220.

information."[123] The Court was not willing to blindly apply the third-party doctrine to any and all types of data exchanged with third parties.[124] Put another way, just because an individual exchanges information with a third party, does not mean it is fully voluntary or informed, especially because cell phones are now so required for everyday life. Instead, the Court was keen to differentiate CSLI data from other types of "non-content" information, such as phone records and bank statements.[125]

Authors Susan Freiwald and Stephen Smith explained how the Supreme Court arrived at its conclusion, namely by considering whether the investigatory techniques were hidden, continuous, indiscriminate, or intrusive.[126] First, the Court determined that acquiring CSLI data was unlike other forms of public surveillance in that it defied societal expectations of how closely one's movements could be monitored and recorded.[127] As mentioned earlier, most people understand that walking about in public is something that can be seen by anyone else around them; on the other hand, most cellphone users do not realize that their device can be used to track their movements minute-by-minute. In Solove's taxonomy of privacy, this investigatory technique falls under the "collection" category.[128] In addition, CSLI data is continuous: it is historically accurate, allowing law enforcement to conduct "near perfect surveillance," "[traveling] back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers."[129] Third, CSLI data is indiscriminate, and records are "continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might be under investigation."[130] In other words, cell phone companies track all of their users all of the time; this kind of data, completely unforeseen by the Constitution's authors, is so large, vast and accessible by law enforcement under the SCA. Lastly, the collection of CLSI data is incredibly cheap and efficient to obtain,

---

123 *Carpenter*, 138 S. Ct. at 2219.

124 Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 223 (2018).

125 *Carpenter*, 138 S. Ct. at 2209.

126 *Id.* at 219.

127 *Id.* at 2270.

128 Solove defines information collection as acquiring data, specifically, the "watching, listening to, or recording of an individual's activities." *See* Daniel Solove*, A Taxonomy of Privacy*, 3 U. PA. L. REV. 470, 490 (2006).

129 *Carpenter*, 138 S. Ct. at 2210.

130 *Id.* at 2218.

adding to easy accessibility.[131] I would argue that these last three factors all fall under Solove's "information processing" category and raise privacy concerns about the way in which amalgamated and stored.

In summary, this decision was significant because it crystallized the Supreme Court's new approach to the reasonable expectation of privacy test under the Fourth Amendment. In doing so, the Court recognized our changing times: that technology necessitated the law to update itself. Interestingly, however, lower courts have been reluctant to extend *Carpenter* to other cases. Why the courts have expressed reluctance and whether they accurately followed *Carpenter's* precedent is an important task to undertake in order to try to understand where Fourth Amendment jurisprudence currently stands.

B. Applying Carpenter to Internet Protocol Addresses

The *Carpenter* decision narrowly addressed CSLI data, and the Supreme Court declined to extend its ruling to other types of surveillance techniques or data.[132] As a result, federal courts have similarly declined to extended *Carpenter* to Internet Protocol ("IP") addresses.[133] As mentioned earlier, IP address cases have been around since the early 1990s, but once the *Carpenter* decision was issued, the legal community was unsure of its reach. At first glance, this result is not surprising: IP addresses differ from CSLI data in several ways.[134]

Every device that accesses the Internet carries a unique number that allows it to exchange information over the Web.[135] The basic purpose of an IP address is to "route" information so that data travels from one computer to another.[136] Each time that data travels from a

---

131 *Id.*

132 *Id.* at 2210.

133 Nathaniel Sobel, *Four Months Later, How Are Courts Interpreting Carpenter?*, LAWFARE (Oct. 18, 2018), https://www.lawfareblog.com/four-months-later-how-are-courts-interpreting-carpenter.

134 CSLI data includes "time-stamped record[s]" of when a cell phone connected to cell sites. *See Carpenter*, 138 S. Ct. at 208. IP addresses, on the other hand, enable computers to connect and share information over the network, as explained in the following paragraph. *See* Josh Fruhlinger, *What is an IP address? And what is your IP address?*, NETWORK WORLD (Nov. 3, 2020), https://www.networkworld.com/article/3588315/what-is-an-ip-address-and-what-is-your-ip-address.html.

135 JAMES GRIMMELMANN, INTERNET LAW: CASES & PROBLEMS 27-28 (9th ed., 2019).

136 *Id*.

computer to a computer, a copy is. However, once "the receiving computer acknowledges that it has received all the data, the sending computer knows that it can delete its own copy."[137] Computers called routers direct the data, which "could potentially be going to any of the billions of computers on the Internet."[138] Routers narrow down which computers to pass along the data to by finding the receiving computer's IP address.[139]

An IP address is a 32-digit binary number,[140] which on its face, appears anonymous. When computer users set up accounts with their Internet service provider (ISP), their IP address is linked to the account holder.[141] IP addresses may also be linked to credit card information, e-mail addresses, web browsing activity, and search engine history.[142] When investigators obtain telephone records, they can only gather information about who an individual has called and when. Similarly, an IP address can show that a transaction of information has occurred, but it also holds a key to a wide range of other personal information.[143]

Here, I argue that, along a spectrum of types of data from "anonymous" to "highly personal," IP addresses have the potential to reveal much more information than telephone numbers or bank checks. For instance, accounts for telephone numbers or banking accounts can each reveal the existence of communications or financial transactions, but IP addresses are the nexus for a much wider range of acts and behaviors.[144] As such, it is difficult to categorize IP addresses because the level of intrusion really depends on what kind of data is linked to them. Investigators may simply use an IP address to identify the account holder, or they can request a user's search history from Google without a warrant.[145]

---

137 *Id*.

138 *Id*.

139 *Id*.

140 *Id*.

141 JAMES GRIMMELMANN, *supra* note 135.

142 Law enforcement must obtain a warrant in order to obtain an individual's web browsing history, but not any of the other pieces of information listed, including e-mail address and search engine history.

143 Jules Polonetsky, *How close to your actual home is the geo-info companies have about your IP address*, FUTURE OF PRIVACY FORUM (July 14, 2009), https://fpf.org/2009/07/14/how-close-to-your-actual-home-is-the-geo-info-companies-have-about-your-ip-address.

144 *Id.*

145 *Transparency Report*, GOOGLE, https://transparencyreport.google.com/user-data/overview (last visited Feb. 8, 2021).

The necessity of Internet use also suggests that the IP addresses are closer to CSLI data than other kinds of non-content information. Like cell phones, Internet use is also widespread and ingrained into almost all aspects of everyday life. Individuals use the Internet and mobile phones to search for jobs, read the news, manage their bank accounts, apply for government benefits, buy everyday household items, in addition to so much more.[146] For many people, Internet use is not optional or occasional. In *Carpenter*, the majority stated that the necessity of a cell phone made it less likely that users were truly aware of cell phone companies' data collection.[147] A similar argument can undoubtedly be made for Internet users.

Lastly, there has been at least one court which has recognized a reasonable expectation of privacy in an IP address. In *State v. Reid*,[148] defendant Shirley Reid logged onto a website from her home computer.[149] The website was owned by a company that had financial dealings with her employer, and while she was on the website, Reid "allegedly changed her employer's password and shipping address to a non-existent address."[150] Eventually, the company reported the IP address and its activities to Reid's employer, who then reported the IP address to local authorities.[151] The local authorities, in turn, issued a subpoena to Comcast, Reid's service provider. Police were informed that the IP address was assigned to Shirley Reid.[152] Although this case was decided in 2008, ten years before *Carpenter*, the New Jersey Supreme Court wrote, "When users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential. Many are unaware that a numerical IP address can be captured by the websites they visit."[153] The Court believed that many Internet users do not fully understand how servers and websites exchanged information with one another—and for those users who *do*

---

146 Brian Frazelle & David Gray, *What the Founders Would Say About Cellphone Surveillance*, ACLU (Nov. 17, 2017), https://www.aclu.org/blog/privacy-technology/location-tracking/what-founders-would-say-about-cellphone-surveillance ("[C]ellphones are essential to modern life. Most of us carry one with us all the time, generating a continuous digital trail of our whereabouts that can reveal intimate relationships, medical conditions, religious practices, political activities, and more.").

147 *Carpenter*, 138 S. Ct. at 2263-64.

148 State v. Reid, 945 A.2d 26, 194 N.J. 386, 2008 N.J. LEXIS 408.

149 *Id.* at 389.

150 *Id.*

151 *Id.*

152 *Id.* at 389-90.

153 *Id.* at 33.

understand what an IP address does, the fact that an IP address is an anonymous number "is the basis for a reasonable expectation of privacy. . ."[154] Unfortunately, however, courts interpreting the aftermath of *Carpenter* have taken a different approach.[155]

C. The Curious Case of Ulbricht

In 2013, Ross William Ulbricht was suspected of running an illegal website called "Silk Road," where he allowed users to buy and sell illegal goods such as illicit drugs.[156] The government obtained a "pen/trap" order pursuant to the Pen/Trap Act.[157] Orders under the Pen/Trap Act do not require probable cause.[158] Under the order, investigators were allowed "to collect IP address data for Internet traffic to and from Ulbricht's home wireless router and other devices that regularly connected to Ulbricht's home router."[159] Upon finding that Ulbricht was responsible for the site, law enforcement convicted him of drug trafficking and several other crimes. [160] He was sentenced to life in prison.[161] The Second Circuit upheld the lower court's decision, rejecting Ulbricht's argument that the pen/trap orders violated the Fourth Amendment.[162]

Ulbricht argued that by accessing his IP address and monitoring his server activity, the government was able to successfully find that Ulbricht operated Silk Road.[163] Moreover, that connection was only made possible by violating an expectation of privacy in his IP address, and that such an intrusion could only be justified by a warrant based on probable cause.[164]

However, the Court rejected this argument. The Second Circuit reasoned that the pen register, which monitored traffic to and from his IP address, was equivalent to a pen register that captures call records, explaining how an IP address is analogous to a telephone number,

---

154 *Id.* at 115.

155 Nathaniel Sobel, *Four Months Later, How Are Courts Interpreting Carpenter?,* LAWFARE BLOG (Oct. 18, 2018), https://www.lawfareblog.com/four-months-later-how-are-courts-interpreting-carpenter

156 U.S. v. Ulbricht, 858 F.3d 71, 82 (2017).

157 18 U.S.C. §§ 3121-27.

158 *Id.*

159 *Ulbricht*, 858 F.3d at 83.

160 *Id.*

161 *Id.*

162 *Id.*

163 *Id.*

164 *Id.*

thereby squarely categorizing IP addresses as "non-content" information.[165] Instead of recognizing how monitoring Ulbricht's IP address was effectively similar to monitoring his web-browsing activity, the Court contended that an IP address merely "indicates the online identity of the communicating device without revealing the communication's content."[166]

After the Court identified IP addresses as non-content information, it then proceeded to discuss the third-party principle and whether Ulbricht had a reasonable expectation of privacy.[167] The Second Circuit reiterated that individuals do not have an expectation of privacy in information they "voluntarily [turn] over to third parties."[168] Internet users know and understand they convey some "numerical information" to the ISP, and that the ISP will record such activity.[169] Anyone who uses e-mail or the Internet, the Court argued, "[relies] on third-party equipment in order to engage in communication."[170] As a result of that reliance on the Internet service provider, users "should know" that Internet traffic is only possible because of their ISP's data collection.[171]

Interestingly, the Court's reasoning was more similar to Fourth Amendment jurisprudence before *Carpenter*, as it emphasized whether the data was exchanged with a third-party, allowing that determination account for the lack of a reasonable expectation of privacy.[172] *Carpenter*, on the other hand, beckoned a multi-factor approach that not only looked at the type of data, but also the method of surveillance.[173] Revisiting the Supreme Court's four factors—whether data collection was hidden, continuous, indiscriminate, and intrusive—it is clear that the type of surveillance conducted in *Ulbricht* falls within Fourth Amendment protection. Because Internet use is so pervasive, data collection is often unbeknownst to users. In *Carpenter,* the Supreme Court worried that cell phone location-tracking data defied users' expectations of how closely their movements could be monitored.[174] There is no reason why cell phone

---

165 *Ulbricht*, 858 F.3d at 84.
166 *Id.* at 85.
167 *Id.* at 97.
168 *Id.* (citing Smith v. Maryland, 99 S.Ct. 2577 (1979)).
169 *Id.* at 96.
170 *Id.* (citing United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)).
171 *Ulbricht*, 858 F.3d at 96.
172 *Id*. at 97.
173 *See generally* Freiwald & Smith, *supra* note 124.
174 *See* Carpenter v. United States, 138 S. Ct. 2206, 2217.

users would not be aware of CSLI data collection, while Internet users should know about data linked to their IP address.

As with CSLI data, internet traffic activity is continuous when the Internet user is on-line. The device may not be carried on an individual's person, but for many, Internet usage does occur daily. Internet activity can also generate a large quantity of data, as dozens of websites can be visited in a single hour. Lastly, like CSLI data, obtaining information regarding the traffic of a certain IP address is cheap and easy, and a large amount of historical data can be recalled quickly by an internet service provider.[175]

Acknowledging that many times IP addresses function as "non-content" data, the courts should understand that some data (like records of traffic to and from websites) may be amassed and assembled in such a way that does provide "content" information. For instance, while law enforcement must obtain a warrant to request a suspect's web-browsing activity, a warrant is not required to obtain an IP address and use a pen/trap order to determine if that address visits a certain website.[176] When a link is made between the device and website server, law enforcement is essentially obtaining information about a user's web-browsing activity without a warrant. In the *Ulbricht* case, data was collected in such way that the "content" of some of his communications were revealed.[177]

In short, while the *Carpenter* Court invited its readers to consider CSLI data in the context of the Internet Age, the Second Circuit does not fully embrace the nuanced and in-depth approach that the former used.

---

175 For example, the U.S. government can request non-content and content information that companies such as Google will produce. *See* 18 U.S.C. § 2709; 50 U.S.C. § 3162; 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-v. *See also United States national security requests for user information*, GOOGLE TRANSPARENCY REPORT, https://transparencyreport.google.com/user-data/us-national-security.

176 18 U.S.C. §§ 3121-27.

177 In other words, Ulbricht's browsing history revealed information that, effectively, revealed content. As David Ingram explains, "Search and browser history can reveal people's personal thoughts like perhaps nowhere else, serving as a kind of electronic confession booth as people put down their guards and stare into phones and computer screens." *See* David Ingram, *Can the government look at your web habits without a warrant? Senators hope to clarify that*, NBC NEWS (May 15, 2020), https://www.nbcnews.com/tech/security/can-government-look-your-web-habits-without-warrant-senators-hope-n1207936.

D. Two Lessons from Ulbricht

There are two lessons that can be gleaned from *Ulbricht*. First, as I have argued in the previous section, the Second Circuit did not properly follow the Supreme Court's precedent. Second, and perhaps more importantly, the refusal to extend *Carpenter* to IP addresses reveals something deeper about the current state of Fourth Amendment jurisprudence—that it provides incomplete and insufficient privacy protections.

Critics of modern Fourth Amendment jurisprudence argue that it is "haphazard"[178] and "illogical"[179] and has failed to keep up with the realities of modern technology.[180] Part of the problem is that the Supreme Court addresses privacy concerns issue by issue, considering each technology, rather than by offering a comprehensive solution and clear guidance as to what types of data are off limits. Additionally, critics have pointed out that the reasonable expectation of a privacy test is far from objective, and there is almost no way to know what exactly is reasonable.[181] People may have different knowledge and literacy of different technologies; as the *Reid* decision pointed out, many Internet users "are unaware that a numerical IP address can be captured by the websites they visit."[182] Similarly, in *Carpenter*, the Supreme Court recognized that CSLI data collection was indiscriminate and that cell-phone users had no real way of consenting to vast data collection. In a world of website cookies, CSLI data, and intangible "data packets" routed all over the world, it is almost impossible that most users can meaningfully consent to data collection.[183] And if they cannot knowingly opt-in, how could they understand when they should or should not expect privacy?

---

178 Solove, *supra* note 21, at 1514.

179 *See* Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1321 (1981).

180 Solove, *supra* note 21, at 1512, 1514.

181 *Id.* at 1521.

182 *Reid*, 945 A.2d 26 at 33.

183 *See generally* Cameron Kerry, *Why protecting privacy is a losing game today—and how to change the game*, BROOKINGS INSTITUTE (Jul. 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/. *See also* Alix Langone, *We Talked to Security Experts About How to Protect Your Online Data. Here's What They Said*, EVERYDAY MONEY (Apr. 17, 2018) ("Because there are no laws preventing companies from doing this, you are essentially helpless when it comes to preventing the sale of your own data even if you are meticulous about avoiding entering important information on computers or phones. . .").

Essentially, the problem with American privacy jurisprudence is that its privacy-as-aegis is premised on the assumption that citizens enjoy strong protections for privacy-as-*tractatio*, when in fact, they do not.[184] Put another way, the "wall" that the Fourth Amendment provides is premised on the assumption that U.S. citizens have some kind of agency over the management and administration of their privacy with private actors.[185] After all, the "reasonable expectation of privacy" test is essentially a question of whether privacy-as-*tractatio* exists. But in reality, those citizens have almost little to no choice but to give up their privacy rights to tech and telecommunications companies, without any kind of legal protections. [186]

Moreover, the reasonable expectation of privacy test does not distinguish between any of the categories of privacy that Solove defined. For instance, the *Ulbricht* court mistakenly only looked at the point at which information was *collected*: the pen/trap order. The invasion of privacy, however, really came afterward: at the point at which it was *processed* and *pieced* together with other data.[187] A similar concern can be seen with automated license plate readers, technology that allows law enforcement to record vehicles' plate numbers and the location and the date at which they were spotted.[188] Viewing publicly displayed license plates is not a privacy violation. Nonetheless, once that data is combined with an extensive record of vehicles' locations and movements throughout time, and *that* combination of data is then *stored* indefinitely, privacy violations have occurred.[189]

---

184 As explained earlier, Fourth Amendment jurisprudence centers on the question of whether the subject of surveillance had a reasonable expectation of privacy. But the ubiquity of data collection, coupled with the lack of federal privacy legislation, has led to citizens unprotected from both corporate and government surveillance. As Daniel Solove explains, the focus on a reasonable expectation of privacy "has led to a contentious jurisprudence that is riddled with inconsistency and incoherence." *See* Solove, *supra* note 21, at 1151.

185 *Id.*

186 As explained earlier, the United States currently does not have a comprehensive privacy legislation akin to the GDPR.

187 As Daniel Solove explains, information processing includes aggregation, "the combination of various pieces of data about a person"; identification, the "linking of information to particular individuals." *See* Daniel Solove, *supra* note 128. In this case, law enforcement combined pieces of data about Ulbricht and linked that information to his identity. *See* U.S. v. Ulbricht, 858 F.3d 71, 82 (2017).

188 *Automated License Plate Readers (ALPR)*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/cases/automated-license-plate-readers (last visited Feb. 8, 2021).

189 *Id*.

Regarding IP addresses specifically, the quality and nature of data can often be shaped by many factors. As explained by Jules Polonetsky of the Future of Privacy Forum:

> [The] real issue isn't really about IP addresses, but rather how to handle information which may be non-personal to one party, but which is linked to personal information in the hands of others. [IP addresses are] often the 'clue' left behind by a someone visiting a website, searching, or creating an email account.[190]

For instance, using an IP address, an individual's search history can also be obtained by either a subpoena or court order, which means that in some cases, investigators can obtain it without a warrant.[191] Furthermore, something as simple as visiting websites can be amalgamated into patterns as behavioral data, which "is stored by companies in large databases that record user activity over time. This data can be linked to an IP address."[192] In addition, "many people often volunteer more personal information by making a credit card purchase, providing an email address, or connecting with that site using their personal online accounts, thus tying their behavioral data to their individual profile more closely."[193] The point here is how much private information an IP address can reveal varies greatly, and therefore, the application of the reasonable expectation of privacy test, as applied in *Ulbricht*, was woefully inept at recognizing this reality.[194]

Solove argues that "[l]ooking at expectations is the wrong inquiry . . . . The law should protect certain information regardless of whether

---

190 Jules Polonetsky, *How close to your actual home is the geo-info companies have about your IP address?*, FUTURE OF PRIVACY FORUM, https://fpf.org/2009/07/14/how-close-to-your-actual-home-is-the-geo-info-companies-have-about-your-ip-address/ (last visited Feb. 8, 2021).

191 *Transparency Report*, GOOGLE, https://transparencyreport.google.com/user-data/overview (last visited Feb. 8, 2021).

192 Dipayan Ghosh & Ben Scott, *Digital Deceit: The Technologies Behind Precision Propaganda on the Internet*, NEW AMERICA (Jan. 28, 2018), https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/.

193 *Id.*

194 *See supra* Sections C & D. For more explanation as to why scholars believe the Fourth Amendment has been applied inconsistency, especially considering new technologies, see Solove, *supra* note 21, at 1511, 1512 (2010) (discussing that "most commentators have recognized that . . . Fourth Amendment doctrine is in a state of theoretical chaos.").

people expect it to be private or not . . . . What matters is what people desire."[195] The European Union's privacy laws, as I explain in the subsequent sections, captures "what the people desire." While the European Union's privacy laws are not without flaws and limitations—it, too, has its critics[196]—we may nevertheless improve privacy laws here in the United States by adopting some of the approaches that European courts have taken.

V. PRIVACY RIGHTS IN THE EUROPEAN UNION

Privacy in European countries has its historical roots in a "distinct set of values and principles" that are quite different than those in the United States.[197] European law considers the "the privacy of personal information [to be] a fundamental right."[198] Many legal scholars agree that the region's support for strong privacy laws emerged from a "desire to prevent a reoccurrence of population control, similar to that exercised by the Nazis during [World War II]."[199] Just as American anxieties of "Big Brother" government animated its zeal for privacy-rooted-in-liberty, Europeans worried that one group could exercise too much control through the information that it amassed on its citizens, like the Nazi party did.[200]

Whitman disagrees.[201] He rather asserts that the ideals of "dignity" and "honor" are rooted much more deeply in European society.[202] Whitman argues that privacy law is part of "a much wider class of legal protections for interpersonal respect,"[203] aiming to "protect people from shame and humiliation."[204] He believes that the privileges of "dignity" and "honor" were initially reserved only for the elite and royal classes in Europe. Over time, however, those privileges were granted to a wider range of people, until they became universally

---

195 Solove, *supra* note 21, at 1524.

196 Niam Yaraghi, *A case against the General Data Protection Regulation,* BROOKINGS (Jun. 11, 2018), https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/.

197 Whitman, *supra* note 10, at 260.

198 *Id.*

199 Michael W. Heydrich, *A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Contract*, 25 BROOK. J. INT'L L. 407, 417 (1999).

200 Levin & Nicholson, *supra* note 18, at 359; Whitman, *supra* note 10, at 1165.

201 Whitman, *supra* note 10, at 1165.

202 *Id*. at 1164.

203 *Id.*

204 *Id*. at 1164-70.

enjoyed by all citizens.[205] Whitman calls this phenomenon "leveling up."[206]

Nevertheless, whether it was due to "leveling up" or fear of population control, respect for one's dignity is enshrined in European law. Article 8 of the European Convention on Human Rights ("ECHR"), titled the "Right to respect for private and family life,"[207] states:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[208]

The European Convention on Human Rights ("ECHR") is an international human rights treaty that has been signed by forty-seven states of the Council of Europe, which is distinct from the European Union,[209] though the two overlap greatly. No country has been admitted to the European Union without first signing onto the Council of Europe.[210] Almost all of the Continental European countries are signatories to the ECHR,[211] which means that the Convention is protected and enforced at both the regional and national levels.[212] The European Court of Human Rights ("ECtHR") is "the ECHR's primary

---

205 *Id.*

206 *Id.* at 1165-66.

207 European Convention on Human Rights, art. VIII. https://www.echr.coe.int/documents/convention_eng.pdf

208 *Id.*

209 *What is the European Convention on Human Rights?*, AMNESTY INTERNATIONAL, https://www.amnesty.org.uk/what-is-the-european-convention-on-human-rights (last visited Feb. 8, 2021).

210 *Id.*

211 Note that the Council of Europe is not the European Union.

212 *The European Convention on Human Rights - how does it work?*, THE COUNCIL OF EUROPE, https://www.coe.int/en/web/impact-convention-human-rights/how-it-works (last visited Feb. 8, 2021).

enforcement mechanism" [213] and provides "a forum for people who believe their rights have been denied" by their national courts.[214] The ECtHR's rulings "legally bind countries to stand by its rulings" and its decisions "influenc[e] the laws and practices of governments across Europe."[215] In other words, European countries' national courts must incorporate ECtHR rulings into their own—and therefore, its rulings on Article 8 and protections of privacy are of great significance to all forty-seven member states. The ECtHR has given Article 8 "wide-ranging interpretation,"[216] applying it cases involving issues ranging from LGBTQ rights[217] to abortion,[218] and as discussed below, unlawful searches and surveillance.

The European Court of Justice ("ECJ"), on the other hand, is the judicial instrument and highest court of the European Union.[219] The ECJ "interprets EU law to make sure it is applied in the same way in all EU countries, and settles legal disputes between national governments and EU institutions."[220] In certain cases, individuals, companies, or organizations can bring cases against EU institutions.[221] The ECJ ensures that all European citizens enjoy the rights under the Charter of Fundamental Rights of the European Union equally. Like the ECHR, the Charter includes privacy rights rooted in the concept of human dignity. For instance, Article 7 guarantees "the right to respect for his or her private and family life, home and communications"[222] and Article 8 protects personal data, declaring that every person enjoys "the right to the protection of personal data concerning him or her."[223]

It is also important to recognize that, of course, each country in Europe has its own privacy laws rooted in its unique history. For

---

213 James, *supra* note 9, at 276.

214 *What is the European Convention on Human Rights?*, AMNESTY INTERNATIONAL, https://www.amnesty.org.uk/what-is-the-european-convention-on-human-rights.

215 *Id.*

216 James, *supra* note 6, at 276.

217 *See* Van Kück v. Germany [2003] ECHR; Oliari and Others v. Italy (2015).

218 *See* A, B and C v. Ireland [2010] ECHR.

219 *Court of Justice of the European Union (CJEU)*, EUROPA, https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last visited Feb. 8, 2021).

220 *Id.*

221 *Id.*

222 Charter of Fundamental Rights of the European Union, art. VII. https://www.echr.coe.int/documents/convention_eng.pdf

223 Charter of Fundamental Rights of the European Union, art. VIII. https://www.echr.coe.int/documents/convention_eng.pdf

instance, Articles 1 and 2.1 of the German Constitution protect citizens' "substantive rights to informational self-determination and the privacy of communications." [224] In France, Article 2 of the Declaration of the Rights of Man and of the Citizen, gives its citizens "a substantive right to respect for their private lives."[225] Ultimately, however, member states of the Council of Europe must abide by the ECHR and Article 8, and the ECtHR has written at-length about Article 8. This Note focuses entirely on ECtHR decisions.

Article 8 of the ECHR protects against both unlawful interference by state actors, as well as one's ability to freely carry out a private life.[226] It should be noted, however, that governmental interference of one's "private life" is acceptable so long as it is "in accordance with the law" and necessary to protect natural security, public safety and the prevention of crime, economic well-being, citizens' health or morals, or for the rights and freedoms of others.[227] The Article's text is wide-ranging and open to interpretation, leaving the door open to exceptions for ideals like "morals" and the prevention of "disorder," which may appear quite disconcerting when compared to the Fourth Amendment. In accordance with the Article's text, when the ECtHR considers whether a government action violates Article 8, it undertakes a two-step test: first, it asks whether the state interfered with the right, and if so, it asks whether the action was based in a domestic law "that is accessible to the general public, [and which] contains specific provisions that preclude arbitrary governmental action and provides citizens with effective notice of any possible incursions into their private information."[228] By focusing on the state's actions, and specifically whether the state interfered with the right to a private life, the Court is able to capture government intrusions that occur in various contexts, including information collection, processing, and more. It also places the burden on the government to ensure that citizens are fully informed of possible violations of privacy rather than assuming every citizen understands and fully consents to data collection practices by private and public actors.[229] The result, I

---

224 James, *supra* note 6, at 260.

225 *Id.*

226 European Convention on Human Rights, art. VIII.

227 *Id.*

228 James, *supra* note 6, at 260.

229 For instance, EU members' "domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. . ." and "must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse..." *See* S. and Marper v. The

argue in the following section, is a much more coherent and comprehensive protection of citizens' privacy.

VI. ARTICLE 8 IN THE DIGITAL AGE

The European Court of Human Rights has addressed privacy and Article 8 in several cases. First and most importantly, the European Court of Human Rights has extended Article 8 protection to "informational privacy [like] online information," including electronic communications.[230] For instance, in *Copland v. United Kingdom*,[231] the Court asserted that European states have a "negative obligation . . . not to interfere with the private life and correspondence of the applicant."[232] In addition to a *negative* duty to refrain from taking certain actions, states also have a *positive* duty to limit data collection.[233] In *S. and Marper v. United Kingdom*, the ECtHR was asked whether Article 8 was violated when police departments throughout England, Wales, and Northern Ireland obtained and retained DNA samples of arrested individuals.[234] These samples were stored in the National DNA Database indefinitely, regardless of whether the arrested individual was ultimately charged or acquitted.[235] While the taking of fingerprints and DNA samples was legally permitted for criminal proceedings in Council member states, the United Kingdom was the only state that permitted "the systematic and indefinite retention of such DNA profiles."[236] In contrast, Scottish police destroyed the DNA samples of arrested individuals who were never charged or convicted.[237] In short, the ECtHR concluded that

---

United Kingdom 1581, Eur. Ct. H.R. 30, para 103 (2008). These provisions mean that the government must take a role in shaping legal safeguards for citizens.

230 Copland v. United Kingdom, App. No. 62617/00, Judgment, 2007-I Eur. Ct. H.R. 253 ("Private life includes the privacy of communications, which covers the security and privacy of mail, telephone, e-mail and other forms of communication; and informational privacy, including online information.").

231 *Id.* at 9.

232 *Id.*

233 Markiyan Bem, *Overview of the recent ECHR case-law related to data protection*, EUROPEAN COURT OF HUMAN RIGHTS (June 17, 2019).

234 S. and Marper v. The United Kingdom 1581, Eur. Ct. H.R. (2008). *See also Factsheet – Personal Data Protection*, EUROPEAN COURT OF HUMAN RIGHTS, https://www.echr.coe.int/Documents/FS_Data_ENG.pdf (last visited Mar. 15, 2021).

235 *Id.* at 3.

236 *Factsheet*, *supra* note 234.

237 S. and Marper v. The United Kingdom 1581, 1581, Eur. Ct. H.R. at 10, para. 36.

Article 8 was indeed violated when biometric data was stored by the state indefinitely. The ECtHR found a violation of privacy *not* at the point of initial data collection, but at the point at which the data was processed improperly.[238]

In its *S. and Marper*[239] decision, the Court made three key points: that Article 8 can be applied in a wide variety of circumstances, that it would apply Article 8 in a precise, fact-specific manner, and that Article 8's ultimate goal is to preserve *personal dignity*. To be more specific, the Court stated that the concept of a private life, as articulated by Article 8, was a "broad term not susceptible to exhaustive definition"[240] and included "the physical and psychological integrity of a person."[241] The Court held that in order to determine whether the information regarded "private-life aspects," it would consider "the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained."[242] Interestingly, the Court's discussion of the *goal* of Article 8 as protecting personal dignity is somewhat reminiscent of the statement in *Katz* that the Fourth Amendment protects "people not places."[243] The ECHR, however, was less concerned about the subjective reasonableness of the defendant and more concerned about whether the defendant would be able to foresee the possibility of surveillance, among other factors.[244] Though not determinative, the foreseeability factor places a greater burden *on the state* to ensure its actions are transparent.

The Court's willingness to extend Article 8 to digital information is further explored in the 2018 case *Ben Faiza v. France*.[245] During an

---

238 *Id.* at 21-25.

239 *Id.* at 28-35. *See also* Markiyan Bem, *Overview of the recent ECHR case-law related to data protection*, EUROPEAN COURT OF HUMAN RIGHTS (June 17, 2019).

240 *Id.* at 20.

241 *Id.*

242 *Id.* at 21.

243 *See Katz v. United States*, 389 U.S. at 351.

244 Katrien Keyaerts, *Ben Faiza v. France: Use of Cell Site Location Information by Police Is Acceptable Interference with Right to Privacy*, 5 EUR. DATA PROT. L. REV. 120, 122 (2019) (discussing how the ECtHR examines whether government actions pass the Article 8 test of possessing "legality, legitimacy, and necessity." "To be allowed under this provision, any infringement must first be 'in accordance with the law', meaning [that the infringement by the government must have] a sufficiently specific and foreseeable legal basis in the internal law of the State.").

245 Ben Faiza v France, 2018-1446/12 Eur. Ct. H.R. The Ben Faiza decision is available in French but not in English. The press release by the ECtHR can however be consulted in English at http://hudoc.echr.coe.int/eng-press?i=003. Also see the

investigation for drug-trafficking, police officers used three distinct surveillance tactics: police officers (1) obtained mobile phone records showing incoming and outgoing calls, supported by a court order, (2) obtained records of defendant's cell tower "pings" from his telephones, and (3) installed a geolocation tracking device to his car.[246] After a 2011 judgement by France's Court of Cassation, the ECHR considered whether any of these three actions violated Article 8. The Court held that Article 8 was violated in regard to the "real-time" geolocation tracking because, "in the sphere of real-time geolocation measures, French law . . . did not at the relevant time indicate with sufficient clarity to what extent and how the authorities were entitled to use their discretionary power."[247] The Court concluded that Ben Faiza "had therefore not enjoyed the minimum protection afforded by the rule of law in a democratic society."[248] On the other hand, the Court held that Article 8 was *not* violated in regard to investigators "obtain[ing] the list of cell towers pinged by the applicant's phone for subsequent tracking of his movements" because it did not involve real-time location.[249] Interestingly, this case is somewhat similar to *Carpenter*; importantly, each court analyzed the *mode* of surveillance, as well as the type of data collected.

In addition, the ECtHR has considered one case regarding Internet Protocol addresses: *Benedik v. Slovenia*.[250] In this case, which was decided the same year as *Ben Faiza*, the Court addressed whether Slovenian police had acted lawfully under Article 8 when they accessed an individual's user information associated with an IP address.[251] Without obtaining a court order, Swiss law enforcement monitored the users of a file-sharing network, one of whom was Benedik, who had shared child pornography over the network. Essentially, Swiss law enforcement used a "pen/trap" order. Benedik was identified after he shared files over the network, and Swiss authorities reported him to Slovenian police.

ECtHR factsheet on personal data protection at https://www.echr.coe.int/Documents/FSDataENG.pdf .-5999245-7685292>.

246 Press Release, *Surveillance measures taken against an individual involved in drug trafficking before Law of 28 March 2014*, EUROPEAN COURT OF HUMAN RIGHTS (Aug. 2, 2018).

247 *Id*.

248 *Id.*

249 *Id*.

250 Benedik v. Slovenia 2018-62357/14 Eur. Ct. H.R.

251 *Factsheet, supra* note 234.

The question before the Court was whether using the IP address to identify Benedik violated his Article 8 right to a private life. In answering this question, the Court found that "the legal provision used by the police to obtain the subscriber information associated with the dynamic IP address had not met the Convention standard of being 'in accordance with the law'" because it "lacked clarity, offered virtually no protection from arbitrary interference, had no safeguards against abuse and no independent supervision of the police powers involved."[252] Essentially, the Court believed the law was overbroad. It considered whether Benedik knowingly gave up his IP address, and whether the state had met its burden of ensuring its laws set clear expectations.

European law successfully protects privacy not just because it emphasizes dignity and examines the potential for violations as data is collected, processed, and disseminated—but also because it has a better grasp of the relationship between privacy-as-aegis and privacy-as-*tractitio*. For instance, in the *Benedik* case, the ECtHR reasoned that unless there was strong privacy-as-aegis—laws that act as a bulwark between the individual and the state—then the Internet user cannot entirely enjoy privacy-as-*tractitio*—the ability to manage one's privacy.[253] As in the *Ben Frazia* case, the Court showed concern for Frazia's inability to enjoy "minimum protection afforded by the rule of law," a shield from unnecessary intrusion by the state.[254] At the same time, it recognized that minimum protection was necessary in the context of unregulated cell phone data collection in which citizens lack privacy-as-*tractitio*. The ECtHR appears to recognize that citizens need to be able to meaningfully consent and manage their data; they need privacy-as-*tractitio*. At the same time, governments must pass laws that have safeguards against abuse and arbitrary use; they must act as effective safeguards against government abuse and ensure citizens' privacy-as-aegis. These two conceptions of privacy work hand-in-hand and are dependent on each other.

VII. CONCLUSION

European courts like the European Court of Human Rights provide a model for American Courts to successfully balance state and

---

252 *Id.*

253 Benedik v. Slovenia 2018-62357/14 Eur. Ct. H.R.

254 Ben Faiza v France, 2018-1446/12 Eur. Ct. H.R.

privacy interests in the digital age.[255] Indeed, by contrasting European and American courts' decisions regarding privacy, we see that not only is U.S. law struggling to provide comprehensive protections for individuals' privacy, but it is struggling to abide by its own precedents. The Fourth Amendment was originally intended to cover a wide range of "unreasonable searches" of citizens.[256] A part of *Katz* picked up on that concept when it stated that the goal of the Fourth Amendment is to protect people. The Supreme Court then took a step in the right direction in *Carpenter*, recognizing that individuals may unknowingly opt-in to data collection practices they do not understand. Unfortunately, American courts are still confined because *Carpenter* was so narrowly tailored, and the reasonable expectation of privacy test is still the hallmark of Fourth Amendment jurisprudence.[257]

European courts, on the other hand, have been able to more quickly adapt to the rapid pace of technological progression. The European Court of Human Rights also looks at the specific contexts of each alleged privacy violation, but it shows much greater concern for whether individuals are able to meaningfully consent to state actions, and whether there are enough checks and balances in state institutions to ensure overreach does not occur. Right now, the primary checks and balances system for Fourth Amendment is the reasonable expectation of privacy test, which places unrealistic burdens on citizens rather than placing those burdens on the government. The U.S. need not adopt every legal principle of the ECtHR, but it would greatly benefit by looking to international and European legal norms and adopting its own version of a test that guarantees privacy in many contexts.

---

255 Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, 28 HARV. HUM. RTS J. 65, 91 (2014).

256 Solove, *supra* note 21, at 1514.

257 *Id.*