Hastings Science and Technology Law Journal

Volume 13
Number 2 *Spring 2022*

Article 6

Spring 2022

Adopting A Legislative Approach for Data in the Fourth Amendment: Defining Personal Data as an "Effect"

Dan Yosipovitch

Adopting A Legislative Approach for Data in the Fourth Amendment: Defining Personal Data as an "Effect"

Dan Yosipovitch*

Abstract

This Article addresses the need to recognize a property-based right in personal data and to limit the amount of personal information that can be lawfully collected about individuals online. The Fourth Amendment, protecting "persons, houses, papers, and effects" from unreasonable searches must be interpreted to ensure privacy for personal data. The evolving nature of data privacy protections and global data privacy standards emphasizes the necessity to develop clear standards and statutes to protect an individual's interest in their personal data. Statutes such as the E.U.'s GDPR and California's CCPA, provide a regulatory framework on how to approach data privacy on the federal level. Using a property-based approach to "effects" and personal data can provide a significant resurgence and revolution in protecting individual privacy. Expanding this privacy right through a legislative approach and the 'mere evidence' rule will reform the convoluted 'reasonable expectation of privacy' framework outlined in Katz v. United States and its progeny.

* I cannot express enough thanks to my research advisor, Professor Harvey Rishikof for his continued mentorship and advice throughout this process. My completion of this project could not have been completed without his expertise and knowledge. In addition, I would like to thank my family and friends for their emotional support.

TABLE OF CONTENTS

I. Introduction

Our personal lives are currently completely exposed online. The personal information accessible online far exceeds the imagination of the Framers' original understanding of current society, and it leaves users far more vulnerable to government exploitation.[1] Digital data, as the court emphasized in *Riley v. California*, is different because "a person can only carry so much on their person . . . [but] with digital cameras people take endless photos and it spans their entire life."[2]

No comprehensive federal legislation exists to protect against the potential governmental monitoring of personal data.[3] The third-party doctrine, which enables the government to search and seize data from third parties without a warrant, allows the government to have substantial reach.[4] Why has Congress neglected to regulate cyberspace? How can one establish property rights for data? Would data even be considered an effect under the Fourth Amendment? All these questions need to be addressed by the current administration. This paper will explain the necessity for statutory protections to limit the amount of personal data collected about individuals.

While some experts believe in the necessity of the third-party doctrine, the introduction of comprehensive federal legislation of data rights similar to the California Consumer Protection Act (CCPA) or General Data Protection Regulation (GDPR), can protect individuals from the largely unrestricted potential exploitation of privacy rights.[5] The California Consumer

1. *See generally* Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L. REV. 4, 796-1149, 982 (2015).

2. 573 U.S. 373 (2014). Oral Argument Transcript at 8–11, 27–29, *Riley*, 573 U.S. 373 (No. 132).

3. CAMERON F. KERRY ET AL., BRIDGING THE GAPS: A PATH TOWARD FEDERAL PRIVACY LEGISLATION, BROOKINGS INSTITUTE (2020); At the time of submission of this article, the American Data Privacy Protection Act (ADPPA) was not introduced to Congress. In July 2022, the ADPPA became the first federal online privacy bill to pass the House Energy and Commerce Committee by a near-unanimous, bipartisan 53 to 2 vote. Nevertheless, even if the bill passes both the House and the Senate, government agencies are exempt and are not subject to compliance with ADPPA regulations.

4. *See* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (providing the benefits of the third-party doctrine). More work is necessary to explore the issues specific to securing one's property, rather than information, to third parties.

5. *See generally* CALIFORNIA CONSUMER PRIVACY ACT, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (hereinafter "CCPA"); EU General Data Protection Regulation (hereinafter "GDPR"): Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 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/EEC (General Data Protection Regulation), 2016 O.J. (L 119) 1; See Laura Jehl & Alan Friel, CCPA and GDPR Comparison Chart, IAPP (2020).

Protection Act and the European Union's General Data Protection Regulation's approaches to data privacy and rights provide a solution to the issue of unreasonable searches and seizures of personal information online.[6] Congress, in legislation, must set forth property-based rights concerning personal data in order to protect personal privacy.

Thesis:

The court ought to consider personal data as an "effect" under the 4th Amendment's search and seizure clause. Moreover, adopting a legislative approach to define an unreasonable search in conjunction with the reasonable expectation of privacy standard from *Katz* should create a new reasonable expectation of privacy.

a. What is an "effect?"

According to Black's Law Dictionary, an effect is, "[p]ersonal estate or property." An "effect" has been held to be more comprehensive than "goods," in that an effect includes fixtures, which "goods" will not include."[7] Under current Fourth Amendment law, there is nothing to recognize personal data as an effect.[8] However, if Congress defines and regulates this form of data to have protection under the Fourth Amendment, it will ensure greater protections for individuals online.[9]

In *United States v. Jones*, the U.S. Supreme Court reintroduced the discussion concerning the "effects" of the Fourth Amendment.[10] Before *Jones*, the court rarely discussed effects or its considerations.[11] The original understanding of "effects" was centered on differentiating protection from moveable goods or property to real property.[12] It was likely limited to personal,

6. *See* CCPA, 2018, Cal. Legis. Serv. Ch. 55 (A.B. 375); GDPR, 2016 O.J. (L 119) 1.

7. *Effects*, BLACK'S LAW DICTIONARY (10th ed. 2014).

8. *See* Brady, *supra* note 1, at 955 (citing Debra Cassens Weiss, *Does Fourth Amendment Protect Computer Data? Scalia Says It's a Really Good Question*, A.B.A. J. (Mar. 24, 2014, 1:06 PM), available at https://www.abajournal.com/news/article/asked_about_nsa_stuff_scalia_says_conversations_arent_protected_by_fourth_a.

9. *See* KERRY ET AL., *supra* note 3.

10. *See* 565 U.S. 400 (2012).

11. Brady, *supra* note 1, at 952.

12. *Id*. at 985; 1 NOAH WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE (New York, S. Converse 1828); 1 JOHN ASH, *Effect*, THE NEW AND COMPLETE DICTIONARY OF THE ENGLISH LANGUAGE (London, Edward & Charles Dilly 1775) (defining "effect" in the plural as "goods; chattels"); N. BAILEY, *Effects*, AN UNIVERSAL ETYMOLOGICAL ENGLISH DICTIONARY (Edward Harwood ed., London, J.F. & C. Rivington et al. 25th ed. 1790) (defining "effects" as the "Goods of a Merchant, Tradesman, &c."); JAMES BARCLAY, *Effect*, A COMPLETE AND UNIVERSAL

rather than real property.[13] The definition of "effects" was guided by state-level sources.[14] Pennsylvania was the first state constitution to reference possessions.[15] It provided "[t]hat the people have the right to hold themselves, their houses, papers, and *possessions* free from search or seizure."[16] Similar statutes were adopted in Vermont, Massachusetts, and New Hampshire.[17]

In addition to state constitutional provisions, members of state ratifying conventions from six states made recommendations that the Federal Constitution include protection for personal property.[18] The initial Fourth Amendment, written by James Madison, included "other property" instead of "effects."[19] However, the committee of Eleven, a committee made up of a delegate from each state, reviewed this proposal, and replaced it with the word "effects."[20] No prior state constitution included the word, and it was the first source to ever include the word as a statute.[21] Although there was no record of the reason for the change from "property" to "effects" most commentators generally agree it was intended to narrow the breadth of the Amendment.[22]

The word "effects", according to early sources, was synonymous with personal property.[23] Modern authorities of dictionaries traditionally cited as the original meaning of the Constitution cites "effects" to mean chattels or possessions.[24] It was a term commonly associated with bankruptcy or inheritance but likely was still defined as personal property.[25]

ENGLISH DICTIONARY (London, J.F. & C. Rivington et al. 1792) (defining "effect" in the plural as "goods, furniture, or moveables").

13. Brady, *supra* note 1, at 948.

14. *Id.* at 982.

15. PA. CONST. of 1776, art X (emphasis added).

16. *Id.*

17. *See* VT. CONST. of 1777, ch. I, art. XI; MASS. CONST. of 1780, pt. 1. XIV; N.H. CONST. of 1784, art XIX

18. *Proposal of Maryland Minority*, Apr. 26, 1788; *Proposal of Massachusetts Minority*, Feb. 6, 1788; *Proposal of Pennsylvania Minority*, Dec. 12, 1787; *Proposal of New York*, July 26, 1788; *Proposal of North Carolina*, Aug. 1, 1788; *Proposal of Virginia*, June 27, 1788.

19. 1 JOSEPH GALES, ANNALS OF CONGRESS, 452 (Washington, Gales & Seaton 1834).

20. H.R. Rep. No. 11, July 28, 1789, reprinted in COGAN, *supra*, n. X , para. 6.1.1.2, at 333-34.

21. *Id.*

22. Brady, *supra* note 1, at 985, n. 175 (quoting Altman v. City of High Point, 330 F.3d 201 (4th Cir. 2003) ("The effect of that change is clear; however, it narrowed the scope of the amendment").

23. *Id.* at 985.

24. *Id.* at 986-87.

25. *Id.*

In *Jones,* the Supreme Court held that law enforcement officers attaching a GPS device on a citizen's car to monitor its movements was a search.[26] Justice Scalia's majority opinion did not apply the *Katz* test, which requires an objective societal and subjective personal reasonable expectation of privacy, in favor of viewing the vehicle as an "effect."[27] The court relied on a textual analysis of the Fourth Amendment.[28] The court held that the standard from *Katz* should be used in "add[ition] to, not substituted for, the common-law trespassory test."[29] Before *Katz*, there was no clear-cut common-law trespassory test.[30] The court found that an individual's Fourth Amendment interests are weak when his property interests are weak.[31]

In an earlier case, *Riley v. California*, the court concluded that law enforcement officers' search of an arrestee's cellphone was illegal.[32] David Leon Riley, a Lincoln Park gang member of San Diego, California, with others, opened fire at a rival gang member who passed by them on the street.[33] Riley was arrested in another vehicle twenty days later, driving on expired license registration tags.[34] He subsequently had his car searched and the police seized his cell phone from his pocket.[35] A detective analyzed the videos and photographs of Riley making gang symbols and signs on the phone to determine if he was gang-affiliated.[36] Riley moved to suppress the evidence regarding his gang affiliation that was acquired through the media on his cell phone.[37]

The court determined that cloud storage raises "the possibility that a search may extend well beyond papers and effects in the physical proximity of an arrestee."[38] In lieu of viewing the cellphone as personal property, the court compared the phone to a house to define the owner's expectations.[39] These distinct holdings and lack emphasize that the court has no clear interpretation of how to consider effects, especially regarding computer data.

26. *Jones*, *supra* note 10, at 413.
27. *Id.* at 406.
28. *Id.* at 404.
29. *Id.* at 409.
30. *Id.*
31. *See* Brady, *supra* note 1, at 948.
32. *Riley*, *supra* note 2, at 403.
33. *Id.* at 373.
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.* at 398.
39. *Id.* at 396-397.

In *United States v. Jones,* law enforcement suspected a defendant of trafficking drugs.[40] They obtained a warrant to install a GPS tracking device on a vehicle belonging to his wife.[41] The warrant required that the device be installed within 10 days and while the vehicle was inside the District of Columbia.[42] Law enforcement acted outside the scope of the warrant by installing the tracking device in Maryland on the eleventh day.[43]

The agents tracked *Jones* for the next four weeks and used that information to prosecute him.[44] The court held that the Fourth Amendment "must provide at a minimum the degree of protection it afforded when it was adopted."[45] The court also held that the *Katz* reasonable expectation of privacy test, "added to, not replaced the common-law trespassory test."[46] Therefore, *Jones* established that trespass on houses or effects is a Fourth Amendment search if the goal of the trespass is to obtain information.[47] However, *Jones* does not set forth a clear outline, of how one can define an "effect" or what constitutes a trespass.[48]

The *Jones* opinion did not define "effects."[49] While the court has devoted significant effort to refine the rest of its search and seizure rules, no decision has clarified how to consider something as an "effect."[50] A few cases note that some things—a parcel,[51] a vehicle,[52] luggage[53] are incontrovertibly effects—and two cases stated "open fields" are not.[54] In one of the footnotes from these cases, the court mentioned that "[t]he Framers would have understood the term 'effects' to be limited to personal, rather than real, property."[55] The cases provide little insight into the identification process of

40. *See Jones*, supra note 10, at 402 (2012).

41. *Id.* at 402.

42. *Id.* at 402-03.

43. *Id.* at 403.

44. *Jones*, *supra* note 10, at 403.

45. *Id.* at 411.

46. *Id.* at 409.

47. *Id.* at 407.

48. Brady, *supra* note 1, at 955.

49. *Id.*

50. *See id.*

51. United States v. Jacobsen, 466 U.S. 109, 114 (1984).

52. *Jones*, *supra* note 10, at 404.

53. United States v. Place, 462 U.S. 696, 705-06 (1983).

54. Oliver v. United States, 466 U.S. 170, 176 (1984); Hester v. United States, 265 U.S. 57, 59 (1924).

55. *Oliver*, *supra* note 54, at 177 n.7.

whether the subject of a search is an effect so that an analysis particular to that classification can begin.[56]

In an analysis of constitutional effects, Professor Brady details two approaches that have dominated the interpretation of effects, the locational privacy approach, and the contextual privacy approach.[57]

The locational-privacy approach dominated most of the Supreme Court's judgments on the issue of "effects" such as in *Florida v. Jardines* & *United States v. Jones*.[58] The locational privacy approach protects against systematic and secretly recorded surveillance of an individual's movements under normal circumstances.[59]

The contextual-privacy approach, primarily followed by state courts, provides more comprehensive insight on how effects should be defined.[60] Some considerations of the contextual approach include the character of the property and space and the duration of separation from owner to property.[61] It does not necessarily matter if the space is public or not.[62] These approaches are more inclusive of personal property and would likely extend these privacy rights to data disclosed to third parties.[63] Yet, this approach has not been adopted by any opinion on the Supreme Court.[64] This may be in part because this approach still does not substantially provide any clearer picture of what can be considered an effect, rather it broadens the scope.[65]

In a comprehensive analysis of effects[66], Professor Maureen Brady advances that an effect should be considered under their own category within the Fourth Amendment.[67] It enables protections above and beyond the protection of things that are not personal property.[68] The court should extend protections to items beyond set on the identifiable person (i.e. a hard drive

56. *See Oliver*, *supra* note 54, at 176; *see also Hester*, *supra* note 54, at 59.

57. Brady, *supra* note 1, at 964, 972.

58. *Id.* at 1014 n.299; *Jones*, *supra* note 10.

59. Brady, *supra* note 1, at 964; *See* Andrew Blumberg & Peter Eckersley, *On Locational Privacy, and How to Avoid Losing it Forever,* ELECTRONIC FRONTIER FOUNDATION (2009), https://www.eff.org/wp/locational-privacy.

60. Brady, *supra* note 1, at 972.

61. *Id.* at 975.

62. *Id.* at 976.

63. *Id.* at 978.

64. *See id.*

65. *Id.*

66. Brady, *supra* note 1, at 946.

67. *See id.* at 998.

68. *Id.*

that was connected to the suspect in question that was accessed remotely).[69] This would place sensitive information, like personal data, on par with the established guidelines outlined in other constitutionally protected areas.[70] In addition, it adds protections for effects in other unprotected circumstances unprotected by other analyses.[71]

Brady suggests the proper approach to assess whether something is an effect should be whether it is "reasonably recognizable" as personal property.[72] Brady argues that a judge is no less suitable to assess what counts as property than the average legislator or person on the street.[73] When examining the court's current understanding of effects, a positivist approach is likely the best solution, because it does not subject a judge to have to make a subjective property decision and analysis of an item as Brady suggests.[74] In the current age, technology has created new types of sensitive information and property, some of which companies have complete control over, such as a user's metadata.

b. *Katz*'s Reasonable Expectation of Privacy Standard

The Constitution protects individuals' right to privacy: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause…"[75] The Fourth Amendment was initially interpreted to protect citizens from government intrusion into homes.[76] Current interpretations "protects people, not places."[77]

The wider interpretation of the Fourth Amendment is not limited to physical intrusions.[78] The Supreme Court has found that a person has a constitutionally protected right in cases where (1) the person must has an actual

69. *Id.* at 999.

70. *Id.* at 999-1000.

71. *Id.* at 1000.

72. *Id.* at 1001.

73. *Id.* at 1002.

74. *See id.*

75. U.S. CONST. amend. IV (emphasis added). This Article need not confront one of the most debated issues in criminal-procedure law: the question of whether the Fourth Amendment requires warrants, operates only to require that searches be reasonable, or functions as some combination of both.

76. *Jones*, *supra* note 10, at 405 ("Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.").

77. Katz v. United States, 389 U.S. 347, 351 (1967) (Harlan, J., concurring).

78. *Id.* at 350.

subjective expectation of privacy; and (2) "the expectation must be one that society is prepared to recognize as "reasonable."[79]

The Supreme Court held in *Katz* that FBI agents need probable cause to obtain a warrant for attaching an electronic recording device on the outside of a public telephone booth.[80] The majority, written by Justice Potter Stewart held that "[t]he Fourth Amendment protects people, not places."[81] Justice John Marshall Harlan, in a concurring opinion, concluded that a person inside a closed phone booth reasonably assumed his calls were not being intercepted.[82] *Katz* relies on whether the individual intended to keep information private and whether that information had previously been disclosed.[83] The current application of the *Katz* test is particularly centered around targeted law enforcement action, rather than warrantless mass data tracking programs, which investigate data to provide some sign of suspicion.[84] A vast majority of Americans expect that their online personal information is collected by the government.[85] When considering disclosures of mass surveillance by their own or foreign governments, which actively collect extensive and vast amounts of communication and internet data, society cannot reasonably expect that all their personal data online is protected and therefore cannot be protected under *Katz*.[86]

The use of biometric databases and mass suspicion-less surveillance tools have become increasingly common by state, federal, and local law enforcement.[87] The *Katz* test does not provide a clear analysis of how this information should be processed.[88] In fact, according to *Smith v. Maryland*, "an individual has no legitimate expectation of privacy in information disclosed to third parties."[89] Nevertheless, Justice Sotomayor recognized in her *Jones* concurrence that this approach is incongruent in the digital age, where

79. *Id*. at 361.

80. *Id.*

81. *Id.* at 352.

82. *Id.* at 360.

83. *Id.* at 352.

84. *Id.*

85. *See* Brooke Auxier, et. al., *Americans and Privacy Concerned Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. PROJ. (2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

86. *See id.*

87. *See* Margaret Hu, Biometric Surveillance and Big Data Governance, in THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW (David Gray & Stephen E. Henderson eds., 2017).

88. *See* United States v. Moalin, 973 F.3d 977 (9th Cir. 2020).

89. 443 U.S. 735, 743-44 (1979).

most of our personal information is disclosed to third parties online, even when disclosing information for mundane functions.[90]

Sotomayor's concurrence agreed with the majority that the *Katz* test did not replace or diminish the common-law trespassory test.[91] She distinguished her reasoning from Justice Scalia's majority in Jones by disputing the constitutionality of warrantless short-term GPS surveillance as a whole, instead of finding the GPS placement as a trespass onto personal property.[92] The information gathered through short-term surveillance can precisely record their every movement and "reflects a wealth of detail about [her] familial, political, professional, religious and sexual associations."[93] Justice Sotomayor distinguished from *United States v. Knotts*, a case heavily cited in the *Jones* opinion.[94]

The *Knotts* case arose over an issue of if whether law enforcement officers, who followed a drug-dealer suspect with a beeper tracking device to a residence, committed an unreasonable search and seizure.[95] The officers tracked a suspect by placing a device on his vehicle and proceeded to search his residence after obtaining a search warrant for the premises.[96] The majority opinion relies on both the 'plain view' and 'open fields' doctrines.[97] The plain view doctrine asserts that one has a lesser expectation of privacy in their car, "because its function is transportation and it seldom serves as one's residence or repository of personal effects."[98] The open fields doctrine allows that the information collected outside an owner's curtilage does not violate the Fourth Amendment.[99] The court emphasized that the facts of the *Knotts* case are different from *Jones* because the officers in *Knotts* had to actively track the suspect in pursuit.[100]

90. *See Jones*, *supra* note 10, at 417 (Sotomayor, J., concurring) (arguing the third-party doctrine is problematic in the digital age).

91. *Id.*

92. *Id.*

93. *See id.* (referencing United States v. Knotts, 460 U.S. 276 (1983)).

94. United States v. Knotts*,* 460 U.S. 276, 276 (1983).

95. *Id.* at 276.

96. *Id.*

97. *See id.* at 281-82.

98. *Plain View Doctrine*, BLACK'S LAW DICTIONARY (10th ed. 2014); *Knotts*, *supra* note 94, at 281 (citing Katz v. United States, 389 U.S. at 361).

99. *Open Fields Doctrine*, BLACK'S LAW DICTIONARY (10th ed. 2014); *Knotts*, *supra* note 94, at 282 (referencing Hester v. United States, 265 U.S. 57 (1924)).

100. *Jones*, *supra* note 10 at 409.

Awareness of governmental surveillance averts individuals from associating with a group and therefore subverts freedom of association.[101] The *Katz* test is inadequate in addressing the significant interest individuals have in protecting their data privacy rights, specifically regarding suspicion-less seizures and the subsequent analysis of mass data programs.[102] By subverting freedom of association, the government is directly infringing on the constitutional right to privacy, regardless if that is expected or not.

c. The Common-Law Trespass Theory of the Fourth Amendment

In *Florida v. Jardines*, Justice Scalia explained for the court that when a government physically intrudes on a person, house, paper, or effect, a search has occurred.[103] In *Jardines*, federal officers brought drug-sniffing dogs onto the premises-based upon a tip that the home was being used as a marijuana grow house.[104] The drug sniffing police dog alerted officers at the front door of the scent of contraband.[105] A search warrant was issued, leading to the homeowner's arrest.[106] The court ruled that the use of a drug-sniffing dog on the premises of a residence constituted an unlawful search.[107] By being physically present on the property/curtilage with a drug-sniffing dog the officers committed an unlawful search because it did not constitute an implied license, like the search of luggage at an airport.[108]

This is regarded as a "trespass" under the "property-based theory" of the Fourth Amendment.[109] In Justice Kagan's concurring opinion she reflected on the nature of drug-detection dogs as a specialized device, similar to the holding in *Kyllo v. United States* which held a search using a highly specialized device as unconstitutional.[110]

In *Kyllo*, a federal agent, suspicious that Danny Kyllo was growing marijuana, used a thermal imaging device to scan Kyllo's residence.[111] The device was used to determine whether the amount of heat from the home was

101. *Id.* at 415 (Sotomayor, J. concurring).

102. *See* Hu, *supra* note 87, 152-53 (2018).

103. 569 U.S. 1 (2013).

104. *Id.* at 1.

105. *Id.*

106. *Id.* at 2.

107. *Id.* at 11-12.

108. *Id.* at 7-8, 10.

109. *See* Ian Samuel, *Carpenter and the Property Vocabulary*, HARV. L. REV. BLOG (2017), https://blog.harvardlawreview.org/carpenter-and-the-property-vocabulary/.

110. *See Jardines*, *supra* note 103, at 12-16 (Kagan, J. concurring); Kyllo v. United States, 533 U.S. 21 (2001).

111. *Kyllo*, *supra* note 110, at 27 (2001).

consistent with the lamps used for indoor marijuana growth.[112] The imaging, along with informants and utility bills led a federal magistrate judge to issue a warrant. Marijuana was found and Kyllo was charged and pled guilty to a federal drug charge.[113] Scalia's majority opinion found that the thermal imaging search was 'presumptively unconstitutional' because it explores details of the home that "would have been previously unknowable without a physical intrusion."[114]

Personal data stored by third parties online exceed far beyond the reach of the original intention and interpretation of the framers of the Fourth Amendment.[115] The federal courts and legislature do not recognize or protect forms of personal data as an "effect."[116] The court has emphasized that a seizure of property happens when government action meaningfully interferes with an individual's possessory interest in that property.[117]

The court did not analyze the *Jones* case under *Katz's* reasonable expectation of privacy test because it was not applicable in a warrantless GPS tracking context.[118] This is because an individual should not expect complete privacy in their movements on public thoroughfares according to the plain view doctrine outlined in *Knotts*.[119] The majority opinion relied on trespass theory, which, as the Court offered as an alternative to *Katz* and provides the basis for Fourth Amendment jurisprudence.[120] The court narrowly held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a [Fourth Amendment] 'search.'"[121]

Before *Katz,* there was no clear-cut common-law trespassory test.[122] The court found that an individual's Fourth Amendment interests are weak

112. *Id.* at 27.

113. *Id.*

114. *Id.* at 34.

115. *See* Brady, *supra* note 1, at 955-56 (citing Debra Cassens Weiss, *Does Fourth Amendment Protect Computer Data? Scalia Says It's a Really Good Question,* A.B.A. J. (Mar. 24, 2014, 1:06 PM), https://www.abajournal.com/news/article/asked_about_nsa_stuff_scalia_says_conversations_arent_protected_by_fourth_a).

116. *Id.* at 955-56.

117. *See Jacobsen*, *supra* note 51, at 113 (1984); Smith v. Maryland, 443 U.S. 735 (1979).

118. *Jones*, *supra* note 10, at 406 (2012) (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

119. *Knotts*, *supra* note 94, at 281.

120. *Jones*, *supra* note 10, at 406-08.

121. *Id.* at 404.

122. *See id*. at 401.

when his property interests are weak.[123] For much of the court's history, a search relied upon whether the government had physically intruded into "persons, houses, papers, and effects."[124]

In *Olmstead v, United States*, government agents wiretapped phone lines running to the defendant's home.[125] The government agents, based on tips of alleged bootlegging in Olmstead's residence, installed wiretaps to listen in at the property without judicial approval.[126] They did not physically enter onto his property, and the court held that there had been no Fourth Amendment "search."[127] Federal officials had wiretaps placed in a suspected bootlegger's building basement without judicial approval, but without trespass upon the property of any of the defendants.[128] The intercepted telephone wiretaps provided investigators with evidence of a conspiracy to transport and import intoxicating liquors.[129] After the government agents uncovered the conspiracy, the suspects were convicted using the evidence obtained by the wiretaps.[130]

The court held that this did not violate the defendant's Fourth Amendment rights because mere wiretapping does not constitute a search and seizure.[131] The majority opinion, written by Chief Justice William Howard Taft, held that searches and seizures refer to an actual physical examination of one's person, papers, tangible material effects, or home and does not include conversations.[132] Although the opinion cited these actions as unethical, the Taft court did not find that this type of evidence should be excluded solely for moral reasons.[133]

Justice Taft utilized the reasoning in *Weeks v. United States*, a case that involved a conviction for transporting lottery tickets through the mail.[134] In *Weeks*, police seized papers and articles, without a search warrant, from the defendant's house after the defendant was arrested.[135] The defendant applied

123. *Id.* at 407.
124. Brady, *supra* note 1, at 952.
125. *See* 277 U.S. 438 (1928).
126. *Id*. at 455.
127. *Id.* at 456.
128. *Id.* at 457.
129. *Id.*
130. *Id.*
131. *Id.*
132. *Id*. at 466.
133. *Id.* at 468.
134. *Id*. at 460 (citing Weeks v. United States, 232 U.S. 383 (1914)).
135. Weeks v. United States, 232 U.S. 383, 386 (1914).

for a court order for the return of his property which the court granted, however, it kept relevant evidence for the case to use at trial.[136] Defendant was convicted and appealed his case claiming the evidence gathered against him was inadmissible under the Fourth Amendment.[137]

The U.S. Supreme Court unanimously reversed, holding in favor of Weeks that this confiscation of evidence was a violation of Fourth Amendment protections and thereby inadmissible.[138] Justice Taft distinguished the Weeks case stating that the wiretaps installed do not constitute a search under the Fourth Amendment and the evidence collected does not deserve constitutional protection.[139] Taft further distinguishes wiretapping from the mail, because sealed mail is delivered by the federal office, which has an explicit constitutional provision and deserves protection.[140] According to the majority for a search and seizure, it must physically occur on the defendant's premises.[141] As a result, an intercepted telephone call does not apply.[142] Justice Taft even makes note that Congress can pass direct legislation to ensure these protections.[143]

Justice Brandeis's dissenting opinion in *Olmstead* argued that telephone lines are a public service that is serviced by an authority.[144] As a result, telephone lines deserve Fourth Amendment protection.[145] He notes that there is no substantial difference between private telephone conversations and a sealed letter.[146] Justice Brandeis finds the invasion of privacy in a private telephone call, "is far greater than that involved in tampering with the mails."[147] He views the majority's opinion as overextending its interpretative reach and failing to account for the future implications of the constitution.[148]

Justice Brandeis cites *Boyd v. United States* as a pillar case for the protection against unconstitutional searches in his reasoning.[149] In *Boyd*, the Court finds that it is a violation of the Fourth Amendment to compel the

136. *Id.* at 387.
137. *Id*.
138. *Id*. at 388-89.
139. *Olmstead*, *supra* note 125, at 461.
140. *Id*. at 464-65.
141. *Id*. at 466.
142. *See id*.
143. *Id*. at 469.
144. *Olmstead*, *supra* note 125, at 471-75 (Brandeis, J., dissenting).
145. *Id.* at 475 (Brandeis, J., dissenting).
146. *Id.*
147. *Id*. at 475 (Brandeis, J., dissenting) (citing *Ex parte Jackson*, 96 U.S. 727 (1877)).
148. *Id.* at 472 (Brandeis, J., dissenting).
149. *Id.* at 472 (Brandeis, J., dissenting) (citing Boyd v. United States, 116 U.S. 616 (1886)).

production evidence from a defendant's residence unless that evidence is contraband, stolen property, or an instrumentality of a crime.[150] This holding is known as the "mere evidence rule."[151] The "mere evidence rule" provides protection against self-incrimination for defendants and is based on the property theory of the Fourth Amendment, however it has been largely overruled in recent case law.[152] Nevertheless, the mere evidence rule can provide insight on how to analyze searches in the modern context in regard to electronic searches.

The court took a broader view in the late 1960s, concluding some non-physical invasions were searches when they invaded the defendant's "reasonable expectations of privacy."[153] Non-physical invasions include wiretapping phone lines like in *Katz* or any other object that has a subjective and objective reasonable expectation of privacy.[154] The government's ability to search or seize items depends on a successful assertion of an interest that was greater than the individual's interest in possession.[155] In the same term that the court held that proving a Fourth Amendment search did not require a physical trespass onto real property, the court expressly abandoned this interest-balancing approach when examining 'effects.'[156] Since the trespass test has never been used, at least in regards to personal data, it is unclear what principles would provide a sufficient basis for the "trespass" portion of the court's test in *Jones*.[157]

The property/trespass theory of the Fourth Amendment, discussed in Justice Scalia's opinion from *United States v. Jones*, found that the placement of a GPS tracking device on Jones' vehicle constituted an unlawful search.[158] Scalia held that the Fourth Amendment protects against trespasses onto personal property.[159]

150. *See* Boyd v. United States, 116 U.S. 616 (1886).

151. *See id*. at 616.

152. *See id*.; *See cf*. Schmerber v. California, 384 U.S. 757 (1966); *Warden v. Hayden* 387 U.S. 294 (1967).

153. *See* Brady, *supra* note 1, at 949; Katz v. United States, 389 U.S. 347 (1967) (Harlan, J. concurring).

154. *See generally* Katz v. United States, 389 U.S. 347 (1967).

155. *Id.* at 372.

156. *Cf. id.* at 373.

157. See Brady, *supra* note 1, at 955 (citing Jones v. United States, 565 U.S. 400 (2012)).

158. 565 U.S. at 404.

159. *Id.* at 404-05.

II. The Judicial Approach

Under the Fourth Amendment, a warrant is not required for personal data from third parties due to the third-party doctrine.[160] The third-party doctrine presumes that information disclosed to a third party is not guaranteed privacy rights and enables the government to collect this information without a warrant.[161]

The third-party doctrine was introduced in two cases, *United States v. Miller* & *Smith v. Maryland*.[162] In these cases, the court established that individuals are not entitled to privacy rights for information disclosed to third parties.[163] These cases decided in the mid-late 1970s came far before the digital revolution and the advent of modern technology.[164] Therefore, they do not adequately address the significant technological shifts or societal implications that have resulted from these advancements.

a. The Third-Party Doctrine (*United States v. Miller* & *Smith v. Maryland*)

In *United States v. Miller*, a 7-2 ruling, the court held that subpoenaing bank records without a warrant did not violate the Fourth Amendment.[165] The majority opinion was written by Justice Lewis Powell, Jr. and joined by Justices Burger, Stewart, Blackmun, Rehnquist, and Stevens.[166] Only Justices Brennan and Marshall dissented. Mitch Miller was charged with carrying alcohol distilling equipment and whiskey on which a liquor tax had not been paid.[167] The Bureau of Alcohol, Tobacco, and Firearms (ATF) subpoenaed bank records which two of Miller's banks complied with.[168] Miller was convicted and appealed his conviction alleging that his Fourth Amendment rights had been violated.[169]

The court's majority relied on *Katz*, stating that, "[w]hat a person knowingly exposes to the public … is not a subject of Fourth Amendment

160. *See generally* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

161. *See generally Miller,* 425 U.S. 435 ; *Smith*, 442 U.S. 735.

162. 425 U.S. 435; 442 U.S. 735.

163. *Miller*, 425 U.S. at 443; *Smith*, 442 U.S. at 744.

164. Douglas Harris, *Carpenter v. United States: How Many Cell Phone Location Points Constitute A Search Under the Fourth Amendment?*, 13 DUKE J. CONST. L. & POL'Y 101, 107-08, 117 (2018).

165. 425 U.S. 437.

166. *Id.* at 435.

167. *Id.* at 437.

168. *Id.*

169. *Id.* at 438.

protection."[170] The opinion reasoned that financial records are not "confidential communications," rather they are negotiable instruments utilized for conducting transactions between the customer and the bank.[171] All the documents seized had information that was "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[172] According to Justice Powell, a bank customer is assumed to have taken the risk when the reveal their affairs to another.[173]

Justice William Brennan's dissent cited *Burrows v. Superior Court*, a California Supreme Court case, which ruled that bank records related to an accused bank account without the benefit of legal process, but with the consent of the bank, were protected under the Fourth Amendment.[174] Brennan found that "the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without obtaining a bank account."[175] Brennan in his dissent highlighted his concerns in the logical and potential extension of the ruling which would enable access to information far beyond bank statements.[176]

In a later case, *Smith v. Maryland*, the court extended the third-party doctrine to phone call records in a pen register.[177] The Supreme Court relied on the *Katz* test again, trying to assess whether there was either a subjective expectation of privacy for phone call records or one that society deems as reasonable.[178] The court, in a 6 to 3 majority, ruled in favor of the state of Maryland's conviction, holding that there was no 'search' under the meaning of the Fourth Amendment.[179] Justice Brennan joined Justices Stewart and Marshall in their dissents.[180]

The defendant, Michael Lee Smith, was charged with the crime of robbery that occurred on March 5, 1976, in Baltimore, Maryland.[181] The victim gave a description of the robber and of a 1975 Monte Carlo observed near

170. *Id.* at 442 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).
171. *Id.* at 442.
172. *Id.* at 442.
173. *Id.*
174. *Miller*, 425 U.S. at 447-48 (citing Burrows v. Superior Court, 529 P.2d 590 (1974)).
175. *Id.* at 451.
176. *Id.*
177. 442 U.S. 735, 745-746 (1979).
178. *Id.* at 740.
179. *Id*. at 745-46 (citing Katz v. United States, 389 U.S. 347 (1967).
180. *Id.* at 746.
181. *Id.* at 737.

the scene of the crime.[182] After the robbery, the victim received threatening phone calls from a man who identified himself as the robber.[183] The police then observed a 1975 Monte Carlo passing by the victim's residence, who fit the robbery suspect details given by the victim.[184] The police then at the request of the telephone company installed a pen register to record the numbers dialed from the telephone at Michael Lee Smith's home.[185] There was no court order or warrant before the pen register was placed.[186] The register revealed that a call was placed from petitioner's home to the victim.[187] At the home, the police found a phone book with the name of the victim and her phone number.[188] The owner and driver of the automobile, Michael Lee Smith, was convicted and challenged his conviction on whether the installation and use of the pen register to collect evidence against him was a 'search' under the meaning of the Fourth Amendment.[189]

The court determined that even if the defendant had a subjective expectation of privacy, "this expectation is not 'one society is prepared to recognize as 'reasonable.'"[190] Because Smith "voluntarily conveyed" the telephone numbers to the company when making a call, he "exposed" the information to the company's equipment in the "ordinary course of business" and should not be protected.[191] Smith "assumed the risk" that the telephone company would reveal these dialed numbers to the police.[192] This ruling further extended the reach of transactional records held by third-party companies to warrantless government seizures.[193]

Justice Thurgood Marshall's dissent emphasized that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[194] Justice Brennan, in his dissent, asserted that it is idle to assume risk where individuals have no practical or realistic alternative.[195] Brennan explains that

182. *Id.*
183. *Id.*
184. *Id.*
185. *Id.* at 737.
186. *Id*.
187. *Id.*
188. *Id.*
189. *Id.* at 738.
190. *Id.* at 743 (quoting *Katz*, 389 U.S. at 361).
191. *Id.* at 743-44.
192. *Id.* at 744.
193. *Id.* at 745.
194. *Id.* at 750 (Marshall, J., dissenting).
195. *Id.*

privacy expectations should be legitimate within the meaning of *Katz*, "not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."[196] Brennan's reasoning raised significant concerns, still at issue when assessing an expectation of privacy in modern times.[197]

b. Revisiting *Carpenter v. United States*: Reforming the Third-Party Doctrine

The third-party doctrine was reaffirmed in the case *Carpenter v. United States*; however, this case limited the scope of governmental intrusion.[198] The plaintiff, Carpenter, argued that the government committed an unlawful search when it collected over a month of his Cell Site Location Information (CSLI) data.[199] The majority, in a 5 to 4 decision, based its opinion largely on *Katz's* reasonable expectation of privacy' framework and *United States v. Jones*.[200] The opinion, written by Chief Justice Roberts, held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements."[201] He was joined in his opinion by Justices Ginsburg, Breyer, Sotomayor and Kagan. Justices Kennedy, Alito, Thomas and Gorsuch filed dissenting opinions.[202]

The data generated in CSLI data is both created by intentional actions (e.g. placing a phone call) or automatically when the phone sends a transmission to the network.[203] Unlike the holding in *Smith*, which found that 'voluntarily conveyed' information is not protected, the court reapplied the *Katz* test and imposed their own interpretation when considering this form of data.[204] The precedents in *Smith* and *Miller* did not adequately address technological advancements regarding personal information and data collected by cell phone location records.[205] Rather, *Carpenter* reaffirms the problematic third-party doctrine and *Katz* framework, only narrowing the scope of what type of personal information can be disclosed.[206]

196. *Id.* at 750.

197. *Id.*

198. *See* Carpenter v. United States, 138 S.Ct. 2206, 2220 (2018).

199. *Id.*

200. *See Jones*, *supra* note 10; *Katz*, 389 U.S. 347.

201. *Carpenter*, 138 S.Ct. at 2217.

202. *See id.* at 2217.

203. *Id.* at 2212.

204. *Carpenter,* 138 S.Ct. at 2216-17 (citing Smith v. Maryland, 442 U.S. 735 (1979)).

205. *Carpenter*, 138 S.Ct. at 2216 (citing Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976)).

206. *Carpenter*, 138 S.Ct. at 2217 (citing Katz v. United States, 389 U.S. 347 (1967)).

In *Carpenter,* the court recognized an individual's interest in protecting their CSLI data from disclosure by third parties.[207] They did not recognize any other legitimate expectation of privacy in any other form of personal data.[208] According to Justice Roberts, "a person does not surrender all Fourth Amendment protection by venturing out into the public sphere." Citing *Katz* Roberts writes that "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." The majority found that allowing government to access cell-site records contravenes that expectation because of the length and breadth of the information collected.[209] Cell-site records were deemed as "being a 'distinct category of information' from other business records."[210]

In Justice Kennedy's dissenting opinion, joined by Justices Thomas and Alito, he argues that cell-site location information should not deserve protection because they are imprecise.[211] In addition, he concluded that these records are created, owned, and controlled by a third party as in *Smith* and *Miller*.[212] Viewing the cell-site records lacked the "requisite connection" to assert a Fourth Amendment property interest.[213] According to Justice Kennedy, these were business records, and the defendants had no reason to believe they were owned and controlled by them. Therefore they were not entitled to have a reasonable expectation of privacy.[214] A business record is one that is created in "the routine, ordinary course of business."[215] Justice Thomas expanded on Kennedy's property argument, emphasizing that because the petitioners had no property interest in the records, they were not entitled to Fourth Amendment protections.[216] His opinion centers on, "*whose* property was searched."[217] He details a textual and originalist argument on property rights under the Fourth Amendment.[218]

Justice Alito's dissent reexamines the meaning of search, stating that retrieving these records was merely an order to look through specified

207. *Id.* at 2217.
208. *See id.* at 2219.
209. *Id.* at 2223.
210. *Id.* at 2219.
211. *Carpenter*, 138 S.Ct. at 2223-25 (Kennedy, J. dissenting).
212. *Id.* at 2226-27.
213. *Id.*
214. *Id.* at 2227.
215. *See id.* at 2227
216. *Carpenter*, 138 S.Ct. at 2235 (Thomas, J. dissenting).
217. *Id.* at 2235.
218. *Id.*

documents and did not require probable cause.[219] Alito views a search as a greater intrusion on personal privacy than simply retrieving cell-site location records.[220] He concurs in his reasoning with Kennedy and Thomas who state that this allows a defendant "to object to the search of a third party's property."[221] He advances his discussion by stating that the warrant requirement does not apply when the government requires records through a compulsory process.[222] Alito considers subpoenas, at most, a 'constructive search' because it does not involve a direct collection of evidence.[223]

The movement towards recognizing rights and protections for personal data by the general public should encourage the courts to shift their adaptation of the third-party doctrine to protect against these concerns.[224]

c. Justice Gorsuch's Dissent in *Carpenter*

Justice Neil Gorsuch's dissent from *Carpenter*, builds upon trespass theory, stating that Carpenter had a property interest in his CSLI data.[225] The dissent emphasizes that the third-party doctrine is almost irreconcilable with the text of the Fourth Amendment.[226] Gorsuch rebuts that the *Katz* test offers the same protections.[227] He stated concerns about whether the *Katz* test would be able to provide any guidance: "We still don't even know what its 'reasonable expectation of privacy' test is."[228]

Justice Gorsuch questioned that if the *Katz* test is determined as a normative question, "why do judges, rather than legislators, get to determine whether society should be prepared to recognize an expectation of privacy as legitimate?"[229] In his dissent, he quoted Justice Scalia's observation that "'reasonable expectations of privacy' come to bear 'an uncanny resemblance to those expectations of privacy' shared by Members of this Court."[230]

219. *Carpenter*, 138 S.Ct. at 2247-61, 2255 (Alito, J. dissenting).

220. *Id.* at 2255.

221. *Id.* at 2247.

222. *Id.* at 2256.

223. *Id.* at 2255.

224. *See generally Carpenter*, 138 S.Ct. at 2214.

225. 138 S.Ct. at 2261-2272 (Gorsuch, J. dissenting).

226. *Id.* at 2268.

227. *Id.* at 2265.

228. *Id.*

229. *Id.*

230. *Carpenter*, 138 S.Ct. at 2265 (Gorsuch, J. dissenting) (citing Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J. concurring)).

Justice Gorsuch emphasized that the *Katz* test produces "often unpredictable—and sometimes unbelievable—jurisprudence."[231]

If the third-party doctrine still applies, personal data could not be protected if it was disclosed to any online third party.[232] However, it does not necessarily eliminate your interest in them.[233] According to Gorsuch, disclosing your papers or letters to a third party does not mean that you should lose all Fourth Amendment protection.[234] Unlike a lifetime of phone and bank records which the *Katz* test permitted the government to search and seize, the court only narrowly limited this as an unreasonable search for the seven days of CSLI data in this case.[235] This distinction does not secure the necessary rights to establish sufficient constitutional protections in one's right to privacy online.[236] It also risks personal data protection because without having complete ownership or property rights over data, an individual would potentially have no claim to privacy protection.[237] Gorsuch implies that data may be considered as an involuntary bailment.[238] "An involuntary bailment is a type of bailment that arises when a person accidentally, but without any negligence, leaves personal property in another's possession."[239] This is rooted in a constitutional originalist understanding of effects.[240]

Federal regulations such as the Children's Online Privacy Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA) prohibit the disclosure of sensitive health information from covered entities.[241] However, there is nothing to protect individuals from the use of the vast amount of personal data that is disclosed to third parties online, such as location information, age, preferences, social/economic status, race, or sexual preference.[242] The *Carpenter* case limits the scope of third-party

231. *Id.* at 2266.

232. *See id.* at 2263.

233. *See id*.

234. *Id.* at 2269.

235. *Id.* at 2266.

236. *Id.*

237. *See id.*

238. *Id.* at 2270.

239. *Involuntary Bailment*, BLACK'S LAW DICTIONARY (10th ed. 2014).

240. *Id.*

241. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

242. *Id.*

disclosures for CSLI data, but its narrow holding barely addresses the vast and comprehensive issues surrounding the disclosure of personal data.[243]

Unlike CSLI, the sensitive nature of some personal records such as health records, mandates higher levels of individual protection. Accordingly, comprehensive federal legislation like HIPPA was introduced to ensure protection. Nevertheless, there is nothing to adequately ensure the protection of personal records not covered under federal statute. Many individuals provide complete access to their phone applications to collect and store the most intimate details of their everyday lives.[244] Without regulations or precedents to protect personal information from being collected by third parties, the government has significant power to collect this information without a warrant and there is no legislation.[245]

d. Defense of the Third-Party Doctrine

Two main arguments are made against the third-party doctrine, which is based on either a doctrinal or functional perspective.[246] Doctrinal claims assert that the Justices are wrong when they state a person does not retain a reasonable expectation of privacy in their third-party information.[247] They claim individuals will often expect privacy rights in this information.[248] The Justices misunderstand privacy because they do not address the difference between exposure to one person and the public.[249] The functional argument is based on the premise that the third-party doctrine extends beyond the reach of the government's power.[250] It provides the police with carte blanche power to access information such as business records, and the prospect of abuses makes it inconsistent with the rights guaranteed under the Fourth Amendment.[251]

Professor Orin Kerr begins by emphasizing the third-party doctrine as a consent doctrine.[252] He partially agrees with the criticisms held by the doctrinal perspective.[253] The court addressed the implications of consent, a year

243. *See* 138 S.Ct. 2206 at 2220.
244. *See Carpenter*, 138 S. Ct. at 2232.
245. *Id.*
246. Kerr, *supra* note 4, at 565.
247. *Id.* at 570
248. *Id.*
249. *Id.* at 571.
250. *Id.* at 572.
251. *Id.*
252. *Id.* at 565.
253. *Id.* at 587.

before *Katz*, in *Hoffa v. United States*.[254] In *Hoffa*, James Hoffa, the president of the Teamsters Union, was tried and convicted for attempting to bribe jury members in an earlier trial.[255] The informant was a local union officer who met Hoffa several times during the first trial.[256] The government had only hired the informant after the first trial.[257]

The court held that so long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid.[258] A person who knowingly discloses information to a third party may be tricked as to what the third party will do with the information.[259] But trickery as to motive or design does not vitiate consent.[260] Kerr embraces this consent-based theory from *Hoffa* but stated that the court departed from these principles in favor of the *Katz* framework.[261] The *Katz* framework fails to adequately address the concept of privacy rights guaranteed to shared spaces.[262] Sharing space or property provides the co-occupant with common authority to permit their consent, but it does not remove all Fourth Amendment protection.[263]

However, there are numerous potential abuses of search that technological advances provide, including the lack of enforceability for internal monitoring.[264] The doctrine enables government officials to utilize spies, informants, bank records, record numbers and obtain billing records all without any cause or court-order in some exceptions.[265] Procedural limitations including: entrapment laws, the Massiah doctrine, internal agency regulations, and First Amendment protections are listed as limiting the government's extension when utilizing the third-party doctrine.[266] Kerr details these Constitutional protections as preventative measures for excessive governmental intrusion outside of the Fourth Amendment.[267]

254. Kerr, *supra* note 4, at 588 (citing Hoffa v. United States, 385 U.S. 293, 303 (1966)).
255. *Hoffa*, 385 U.S. at 296.
256. *Id.* at 298.
257. *Id.*
258. *Id.* at 302
259. *Id.* at 303
260. *Id.*
261. Kerr, supra note 4, at 589 (citing *Hoffa,* 385 U.S. at 303).
262. *Id.*
263. *Id.* at 590.
264. *Id.*
265. Kerr, *supra* note 4, at 590.
266. *Id.*
267. *Id.*

Entrapment law, a judicially created doctrine, although recognized by statutes in some states, regulates how the police can utilize secret agents.[268] If the police target an innocent person, the undercover officer cannot induce the target into committing a crime. However, Kerr does not discuss data-related concerns.[269] Although specific individuals may not be entrapped, by the police there are significant interests in protecting information that is not criminal in nature.[270] Nevertheless, entrapment law still adequately regulates abusive law enforcement practices in how they pressure innocent defendants.[271] Although the use of secret agents may not extend to mass government surveillance programs, their use still raises significant concerns about how the government can manipulate and coerce information from its citizens online.[272]

The second defense against the functional perspective is the Massiah doctrine.[273] In *Massiah v. United States*, the Supreme Court held that an agent of the government cannot question a person who has been charged with a crime.[274] In this case, the court found that a defendant's statements to a codefendant, while on bail, in the absence of counsel, were inadmissible.[275] The statements, made by Massiah to a codefendant, who unbeknownst to Massiah was a government informant, were inadmissible because they violated his Sixth Amendment rights.[276] Agents had bugged the codefendant Colson's car and directed Colson to discuss his crimes with Massiah.[277] An agent listened in on the conversation and heard Massiah's incriminating statements.[278] The court found that even though Colson was a confidential informant who provided the information, he met the criteria of an "agent."[279]

The court in *Massiah* found that a person indicted on criminal charges has a constitutional right to have an attorney present during police interrogations.[280] Relying on a totality of circumstances approach, the court found that

268. *Id.* at 591.
269. *See id.*
270. *Id.* at 592.
271. *Id.*
272. *Id.*
273. *Id.* at 592 (citing Massiah v. United States, 337 U.S. 201 (1964)).
274. *See* 337 U.S. 201, 207 (1964).
275. *Id.* at 203-204, 207.
276. *Id.*
277. *Id.* at 202-203.
278. *Id.* at 207.
279. *Id.* at 206
280. Kerr, *supra* note 4, at 592-93 (citing Massiah v. United States, 337 U.S. 201 (1964)).

the defendant's Fifth and Sixth Amendment rights were violated because his statements were deliberately elicited.[281] Entrapment law protects against how the government may approach a suspect on the front end of an investigation, the *Massiah* doctrine protects suspects at the end of the process.[282]

The First Amendment protects overreaching investigations by requiring a good faith reason for doing so.[283] The good faith test addresses a significant concern because it protects individuals who fear investigations are targeted against individuals who exercise their First Amendment rights.[284] The Ninth Circuit explained the use of secret agents is permitted only when it is "justified by a legitimate law enforcement purpose that outweighs any harm to First Amendment interests."[285]

The more the government can collect, without proper cause or court order about individuals, the less transparency there is about what is collected.[286] Therefore, it is imperative for data privacy regulations to address the significant implications of what can and cannot be collected.

III. The Legislative Approach: What is Personal Data?

a. The E.U.'s Approach: General Data Protection Regulation (GDPR)

When considering 'personal data' as an "effect", the courts should consider a progressive statutory definition of personal data:

The GDPR's definition of personal data is:

> '[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[287]

281. *Id.* at 593

282. *Id.*

283. *Id.* at 593-94

284. *Id.* at 594

285. *Id.*

286. *Id.* at 594 (quoting *cf.* NAACP v. Alabama ex. Patterson, 357 U.S. 449, 462 (1958) (Invalidating an Alabama production order intended to prevent NAACP members from conducting further business in the state)).

287. Regulation 2016/679 of Apr. 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1, 33 (EU) [hereinafter GDPR].

Data protection is recognized as a fundamental right according to the Charter of Fundamental Rights of the European Union.[288] The protections are specifically concerning the processing of personal data.[289]

The GDPR addresses these principles when processing personal data: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.[290] It requires permission by the data subject to the use of their personal data.[291] It specifically regulates personal data to ensure a significant number of protections and remedies for individuals whose information is exposed.[292] It does not protect data of "legal persons."[293] Therefore, the personal data of companies or data related to the deceased are not considered personal data in most cases under the GDPR.[294] Any information entails both "objective" information like an individual's height and "subjective" information like employee evaluations.[295]

This information is not limited to a specific medium or format.[296] Even information that is inaccurately attributed to an individual is considered personal information under the GDPR.[297] Personal data can identify an individual either directly or indirectly.[298] An individual is directly identifiable if one can identify them using only the information possessed.[299] Indirect identifications occur when one cannot identify them solely on the given information, but the information can be combined with other information reasonably accessed from another source to make an identification of the individual.[300] Even processing information that may have an effect on the individual or is related to the individual is considered personal data.[301] Also, information that does not qualify as personal data for one person may be considered personal data for another party.[302] For example, a photo of a street made by a

288. 2016 O.J. (C 202) p. 395.
289. *Id.*
290. GDPR, *supra* note 181 at Chapter 2, Art. 5-11.
291. *Id.* at 37.
292. *Id.* at 35-36.
293. *Id.* at 39.
294. *Id.*
295. *Id.* at 38.
296. *Id.* at 36.
297. *Id.* at 35.
298. *Id.*
299. *Id.* at Chap. 1.
300. *Id.*
301. *Id.* at 5.
302. *Id.*

photographer is not personal data, however, that photo in an investigator's who is working to identify who was present on that street at that time likely is.[303]

b. California's Approach: California Consumer Protection Act (CCPA)

The California Consumer Protection Act (CCPA) defines personal data as personal information:

> "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:[304]

According to the CCPA, an individual's personal information is only protected against businesses that meet any of the following: have gross annual revenue of over $25 million; buy, sell or receive personal information of over 50,000 California residents, households or devices or derive more than 50% of their revenue from selling California residents' personal information.[305]

Unlike the GDPR, the CCPA does not apply to government agencies or nonprofit organizations.[306] Individuals may only file claims of data breaches against businesses and have to include personal information that has specific identification.[307] The breach must have included your first name (or initial), last name, and another identifier such as your social security number or driver's license number in a nonencrypted and nonredacted form.[308]

The CCPA permits California residents to have four rights to their data.[309] The *right to know* about the personal information a business collects about them.[310] The *right to delete* that information.[311] The *right to opt-out* of the sale of their personal information and the r*ight to non-discrimination* for

303. *See id.*

304. Cal. Civ. Code § 1798.140 (o)(1) (West 2020).

305. § 1798.140 (c)(1)

306. *See* General Data Protection Regulation, *supra* note 287; Cal. Civ. Code § 1798.140 (c)(1) (West 2020).

307. Cal. Civ. Code § 1798.150 (West 2020).

308. Cal. Civ. Code § 1798.100 (West 2018).

309. Cal. Civ. Code § 1798.100 - 199.100. (West 2018).

310. Cal. Civ. Code § 1798.115 (West 2018).

311. Cal. Civ. Code § 1798.105 (West 2018).

exercising their CCPA rights.[312] Individuals can submit requests for businesses to provide information about what they collect about them.[313] However, businesses are permitted to refuse to disclose the information for a variety of reasons.[314]

An individual can request to know what personal information is collected about them. The business report would provide a comprehensive report of information collected about the individual.[315] However, businesses have significant flexibility to reject these requests due to a plethora of exceptions.[316]

The third right guaranteed under the CCPA is the opportunity to opt-out of the sale of personal information.[317] Individuals can request that their information not be sold by the business without prior authorization.[318] Children under 16 are automatically opted out but can opt-in if they elect to.[319]

Also, the CCPA permits individuals to request that their information be deleted.[320] Nevertheless, the CCPA carves out numerous exceptions, such as if the business needs the information to comply with their own warranties or safety measures to permit businesses to deny the requests to delete personal information.[321]

Certain forms of personal data should be secured the same rights as "houses, papers, and effects" because they implicate the same constitutional concerns.[322] An individual's entire life and information is almost entirely stored on their devices, on the cloud, and by third parties.[323] Without protections to ensure the safety of this information, it leaves the government capable of extracting all the information without knowledge or consent of the users.

The information that is accessible online, leaves individuals vulnerable to the will of third parties according to the present interpretation of the third-

312. Cal. Civ. Code § 1798.120-125 (West 2018).

313. Cal. Civ. Code § 1798.100 (West 2018).

314. Cal. Civ. Code § 1798.148 (West 2018).

315. *See* Cal. Civ. Code § 1798.100 (West 2018).

316. *See* Cal. Civ. Code § 1798.148 (West 2018)

317. *See* Cal. Civ. Code § 1798.120 (West 2018)

318. *Id.*

319. *Id.*

320. *See* Cal. Civ. Code § 1798.125 (West 2018)

321. Cal. Civ. Code § 1798.145 (West 2018)

322. *See* Alan Z. Rozenshtein, *Fourth Amendment Reasonableness after Carpenter*, 128 YALE L.J. 943, 951-53 (2019).

323. *See id*.

party doctrine and statutes.[324] Without any significant federal oversight on the personal information collected about individuals, the public is subject to wait until a privacy right is recognized.[325] Nevertheless, the court should recognize that not all personal data should be protected and therefore it is unnecessary to subject all forms of personal data to a determination of a reasonable expectation of privacy.[326]

IV. Defining Personal Data as an Effect

The first theory of property rights stems from Enlightenment philosophy, which believes property is an individual's natural right.[327] The core belief is the idea that civil society was created on the basis of property.[328] Individuals seek to protect the things they own.[329] Civil society provides a system of rights, protections, and liberties to protect ownership by the individual.[330] However, these property rights are outside of the realm of societal constructs.[331] A pre-state of nature is the foundation of an individual's ownership over personal property.[332] Individuals have a natural right to own the fruits of their labor.[333]

As John Locke argued, "an apple on the tree is of no use to anyone—it must be picked to be eaten—and the picking of that apple makes it one's own."[334] In the context of data, individuals have a natural right to the ownership of their identifiable traits and information. Also, individuals should have natural ownership over the work they provide to third parties. Individuals submit their "labor" by typing up searches or filling out information almost every day online.[335] Companies have a significant interest in the labor and information that individuals' data can provide.[336] As a result, there is an

324. *Id.*

325. *Id.*

326. *See id.*

327. Richard A. Epstein, *Property Rights, State of Nature Theory, and Environmental Protection*, 4 N.Y.U. J. L. AND LIBERTY 2-3 (4:1 2009).

328. John Locke, *Two Treatises of Government*, ed. Peter Laslett (Cambridge: Cambridge University Press, 1988) 137-139.

329. *Id.*

330. *Id.*

331. *Id.*

332. *Id.*

333. *Id.*

334. *Id.*

335. *See* Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 222 (2018).

336. *Id.* at 242.

inherent right to keep ownership of their labor and subsequent data.[337] It is imperative to create safeguards to prevent unlimited exposure to personal information exposed online.

Personal data is considered as a fact under intellectual property law, and therefore is not copyrightable.[338] Although data reflects a fact collected on a user, it deserves protection because individual information is more sensitive and significant than a mere fact.[339] It directly reflects an individuals' identity, decisions, and tendencies. It is not derived solely from actual content but influenced by the surrounding circumstances. To properly consider data in the current legislative framework under intellectual law, it should be viewed as a tangible matter and deserves a property-based right.[340]

To protect against unreasonable searches, personal data should advance the current efforts to regulate personal data set forth by the CCPA and GDPR, while emphasizing the foundational property-based principles protected under the Fourth Amendment.[341]

When considering if personal data is protected under the Fourth Amendment, legislatures should consider adopting a statutory framework that embraces personal data as real property.[342]

A potential statute may include language as follows:

> Personal data is a form of real property and tangible matter that is covered under Constitution. Any data reasonably linked to a natural person, is protected against unreasonable searches and seizures and unnecessary governmental intrusion. Electronic forms of personal data cannot be compelled for production unless that evidence is contraband, stolen property, or an instrumentality of a crime.[343]

In comprehensive data regulations, many states ensure the data subject the right to know, request, control, and delete their personally identifiable information.[344] By adopting a mere evidence rule for personal data, legislators would intend to create a quasi-real property right.[345] Creating these statutes provides notable safeguards to protect one's right to privacy in the

337. *Id.* at 226-27.
338. *Id.* at 267.
339. *Id.* at 226-27.
340. *See id.* at 262-63.
341. *See id.* at 252.
342. *Id.*
343. *See id.*
344. *Id.* at 266-70.
345. *Id.*

digital age and prevent the wanton accumulation of personally identifiable information.[346] Unlike in *Schmerber v. California*, which found that warrantless searches that intrude the human body (such as blood samples) are constitutional, a person's online profile is far more intrusive.[347] It can provide insight into the most sensitive levels of information about an individual, their interests, their health, and location.[348] By limiting the scope of warrantless seizure of personally identifiable information online, the fourth amendment right to privacy can remain intact.[349] If neglected, American citizens are subject to the goodwill of domestic and foreign to utilize this information properly.

a. The End of the E.U.- U.S. Privacy Shield: Schrems II

The Court of Justice of the European Union (CJEU) ruled in *Schrems and Facebook Ireland v. Data Protection Commissioner* ("Schrems II"), that international data flows under the European Union's comprehensive data reform, the General Data Protection Regulation (GDPR).[350] The CJEU found that the EU-US Privacy Shield does not provide adequate protection and therefore is invalidated.[351]

Maximillian Schrems, an Austrian data privacy activist, filed a case against Facebook, Ireland in 2013 for failing to protect the privacy interests in his Facebook data.[352] This lawsuit stemmed from concerns of U.S. surveillance that were exposed in the Snowden whistleblower scandal in 2013.[353] Schrems argued that the E.U. should prohibit the transfer of data to the U.S., because of Facebook USA's alleged involvement in the NSA's PRISM Mass Surveillance program.[354] This mass surveillance program is

346. *See id.*

347. *See id*.; *see Schmerber*, *supra* note 152.

348. Daniel J. Solove & Paul Schwartz, *Reconciling Personal Information in the United States, and the European Union*, 956 GW LAW FACULTY PUBLICATIONS & OTHER WORKS 1, 4-6 (2013).

349. *See id*.

350. CJEU Case C-311/18, Schrems and Facebook Ireland v. Data Protection Commissioner (hereinafter "Schrems II") (2020).

351. *Id.* at 176.

352. Hunton Andrews Kurth, *BREAKING: Unexpected Outcome of Schrems I Case: CJEU Invalidates EU-U.S. Privacy Shield Framework but Standard Contractual Clauses Remain Valid* (2020), https://www.huntonprivacyblog.com/2020/07/16/breaking-unexpected-outcome-of-schrems-ii-case-cjeu-invalidates-eu-u-s-privacy-shield-framework-but-standard-contractual-clauses-remain-valid/.

353. *Id.*

354. Genna Churches & Monika Zalnierute, "*Contracting Out" Human Rights in International Law: Schrems II and the Fundamental Flaws of U.S. Surveillance Law*, HARV. INT'L L.J. (2020),

responsible for collecting vast and extensive amounts of information on users of online platforms. He advocated that Facebook needed to guarantee "adequate protection" for its data transfers to non-EU countries.

The case was initially filed in Ireland then officially referred to the CJEU, which decided the case in 2015. The Schrems II case originated from that 2015 CJEU decision in *Maximillian Schrems v. Data Protection Commissioner* ("Schrems I").[355] *Schrems I* is responsible for invalidating the E.U.-U.S. Safe Harbor decision for the international transfer of personal data.[356] The E.U.-U.S. Safe Harbor framework from 2000 provided principles for American companies to comply with when transferring data from the E.U. to the U.S. such as: notice, choice, onward transfer, security, data integrity, access, and enforcement.[357] It allowed US data transporters to self-certify that they provided "essentially equivalent" protection as E.U. law requires.[358]

In *Schrems II,* the Irish Data Protection Commission made an argument that the Standard Contractual Clauses (SCCs) for the transfer of personal data to processors outside the EU did not have an adequate level of protection of personal data.[359] These SCCs are contract clauses that ensure data privacy protections as "essentially equivalent" to E.U. law.[360] The SCCs stated: The CJEU concluded that these clauses lacked safeguards against U.S. government surveillance and therefore violate the EU Charter of Fundamental Rights.[361] The *Schrems II* decision emphasizes the significance of data protection on global trade and the role privacy professionals play in implementing adequate protections with foreign legal requirements.[362] The CJEU reaffirmed the validity of SCCs, but they must comply with GDPR standards.[363]

---

https://harvardilj.org/2020/08/contracting-out-human-rights-in-international-law-schrems-ii-and-the-fundamental-flaws-of-u-s-surveillance-law/.

355. CJEU Case C-362/14, Schrems v Data Protection Commissioner (hereinafter "Schrems I") (2015).

356. *Id.*

357. *Id.*; European Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles (2000).

358. Case C-311/18, Schrems II (2020) CJEU.

359. *Id.*

360. *Id.*

361. Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and National Security*, BROOKINGS INSTITUTE (2020), https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.

362. Case C-311/18, Schrems II (2020) CJEU.

363. *Id.*

Companies and regulators must conduct a case-by-case analysis in determining whether foreign protections concerning government access to transferred data comply with E.U. standards.[364] The CJEU stated that SCCs must implement appropriate safeguards, enforceable rights, and effective legal remedies.[365] When companies do not comply, National Data Protection Authorities must provide additional safeguards or cease transferring their data.[366] The decisions to suspend these transfers are reviewed on a case-by-case basis.[367] However, the CJEU held that these authorities cannot act to suspend, limit, or ban these data transfers when the Privacy Shield is enforced.[368]

This decision invalidated the E.U.-U.S. Privacy Shield for two main reasons. The court found that U.S. surveillance programs are not limited to what is 'strictly necessary and proportional' as required by E.U. law.[369] Therefore, they do not meet the requirements of Article 52 of the EU Charter on Fundamental Rights. Article 52 states that "[a]ny limitation on the exercise of the rights and freedoms… must be provided for by law and respect the essence of those rights and freedoms."[370] Schrems argued that exposing the personal data of E.U. citizens risks the fundamental human right to privacy.[371]

Secondly, the court determined that concerning U.S. surveillance, E.U. data subjects do not have sufficient actionable judicial redress and do not have the right to an effective remedy under U.S. law, as required by Article 47 of the E.U. Charter.[372] The vast reach of U.S. surveillance programs, lack of an individual's ability for independence, and remedies available by transferring data to the US make the EU-US Privacy Shield incompatible with current E.U. standards.[373] The CJEU held that surveillance programs like PRISM and UPSTREAM which are based on Foreign Intelligence Surveillance Act (FISA) section 702, are not narrowly limited to data that was strictly necessary for foreign intelligence.[374] These programs collect data

364. *Id.*

365. Churches & Zalnierute, *supra* note 354.

366. *Id.*

367. *Id.*

368. Case C-311/18, Schrems II (2020) CJEU.

369. *Id.*

370. O.J. C. 202, Article 52, 7.5.2016, p. 391-407.

371. Case C-311/18, Schrems II (2020) CJEU.

372. Caitlin Fennessy, *The 'Schrems II' decision: EU-US data transfers in question*, IAPP (2020), https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

373. *Id.*

374. Churches & Zalnierute, *supra* note 354.

from undersea cables or providers like Google and Facebook.[375] They provide no actionable rights in protecting their data and consequently have no real remedy if privacy rights are violated.[376] As a result, the court found that the Privacy Shield Decision could not ensure an "essentially equivalent" protection of personal data guaranteed by the GDPR and should be regarded as invalid.[377]

This ruling leaves many questions unanswered. Many companies, data controllers, and exporters are now asking how data can lawfully be transferred from the EU to the United States or any other country outside the E.U.[378] Data privacy experts need to comply with the GDPR and the national security interests of E.U. member states.[379] The CJEU's findings make it seemingly impossible to transfer data lawfully from the E.U. to the U.S.[380] Some individuals argue that not all organizations are subject to U.S. Surveillance.[381] Nevertheless, the CJEU's findings make it seem likely that the adequacy of protection from surveillance by any company is sufficient.[382]

Companies can play a role in protecting human rights in international law, however, regarding data protection, contractual clauses are not sufficient due to the extensive powers given to the U.S. authorities for surveillance.[383] There are limited efforts by the U.S. government to contract to comply with these policies.[384] Currently, there are only a few specific pieces of legislation on foreign surveillance programs, but these programs are typically authorized by a supervisory body or by executive order.[385] Although the Snowden revelations and calls by the E.U. parliament revitalized talks in U.S. Congress for reform, these conversations have now stalled.[386] Without significant changes to U.S. Surveillance policy, there is likely no way to adequately ensure proper compliance with the GDPR.[387] This likely will lead

375. *Id.*

376. Lucie Fournier & Christopher Schmidt, *Schrems II Confirms Validity of EU Standard Contractual Clauses, Invalidates EU–U.S. Privacy Shield*, JONES DAY (2020), https://www.jonesday.com/en/insights/2020/07/schrems-ii-confirms-validity.

377. *Id.*

378. *Id.*

379. *See id.*

380. Churches & Zalnierute, *supra* note 354.

381. *Id.*

382. *Id.*

383. *Id.*

384. *Id.*

385. Meltzer, *supra* note 361.

386. Churches & Zalnierute, *supra* note 354.

387. *Id.*

to numerous suits by privacy advocates to challenge the transfer of their data overseas.[388] Without significant reform, tech companies might have to process personal data in Europe, because contracting out protections against infringements on data privacy rights are highly doubtful.[389]

The European Union issued new guidelines and guidance to govern data transfers to foreign countries. However, because the privacy shield was invalidated, the current state of data transfers between the U.S. and E.U. is in limbo.[390] The European Data Protection Board has implemented some supplementary measures to manage these transfers.[391] These supplementary measures fall under three categories: technical, contractual and organizational.[392] While these supplemental measures provide a path forward, they do not provide an adequate or comprehensive enough solution for all data transfers.

Positivism recognizes the law is whatever society dictates.[393] The recognition of the law depends on what society chooses.[394] Law is a matter of what is ordered, decided, practiced, and tolerated.[395] It does not matter whether the law is just or unjust, it only matters if society or a governing body considers it valid or not.[396] Positivists believe there is a connection between law and the common good, but the law might not always reflect it.[397] Regarding personal data, there is no U.S. federal regulation, however, the Schrems II ruling provides a significant societal schism to recognize personal data as something worth protecting.[398] It is in the best interest of all parties, in the E.U. and U.S. to recognize similar data protection rights to ensure compliance with international trade laws and national security issues.

a. A New Notice Requirement? Analyzing *United States v. Moalin* (2020)

While not all forms of data need to be protected, the vast amounts of information collected online could lead to problematic results. Most of our

388. *Id.*

389. *Id.*

390. *Id.*

391. *Id.*

392. *See id.*

393. Leslie Green & Thomas Adams, *Legal Positivism,* THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., 2019) https://plato.stanford.edu/archives/win2019/entries/legal-positivism/.

394. *Id.*

395. *Id.*

396. *Id.*

397. *Id.*

398. Meltzer, *supra* note 361.

personal information online is already compromised and accessible to the government on a massive scale.[399] In 2020, the Ninth Circuit in *United States v. Moalin*, a case concerning the NSA's metadata collection program, determined that the United States government unconstitutionally collected information about its citizens.[400]

The case concerns U.S.-Somali nationals, who sent or conspired to send $10,900 to Somalia to support a foreign terrorist organization.[401] The Ninth Circuit found that the NSA's telephony metadata activities may have violated the Fourth Amendment of the United States Constitution and violated the Foreign Intelligence Surveillance Act (FISA) when collecting telephony metadata of at least one of the defendants.[402] The Ninth Circuit confirmed that the Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter evidence or use information obtained or derived from a government's foreign intelligence authorities.[403] The defendants' convictions were affirmed because the lack of notice did not prejudice them, thus suppression was not warranted.[404] Most significantly, the Ninth Circuit found that the metadata collected on millions of Americans was unconstitutional.[405]

The Ninth Circuit included that there might be a new obligatory notice requirement for the Fourth Amendment.[406] The opinion concluded that the government is only required to "inform the defendant that surveillance occurred and that the government intends to use the information or derived from it."[407] Furthermore, the "Fourth Amendment requires that a person subject to a government search receive notice of the search, absent "exigent circumstances."[408] In prior cases, the constitutional notice requirement only

399. *See id.*

400. *Moalin, supra* note 88.

401. *Id.* at 983-86.

402. *Id.* at 996-98.

403. *Id.* at 984-85.

404. *Id.*

405. *Id.* at 996.

406. *See* Orin Kerr, *Did the Ninth Circuit Create A New Fourth Amendment Notice Requirement for Surveillance Practices?,* LAWFARE (2020) (citing United States v. Moalin, 973 F.3d 977 (9th Cir. 2020)), https://www.lawfareblog.com/did-ninth-circuit-create-new-fourth-amendment-notice-requirement-surveillance- practices.

407. *Id.*

408. *Moalin*, *supra* note 88, at 999 (citing Berger v. State of New York, 388 U.S. 41, 60 (1967)).

required the United States Government to leave notice only when a warrant was executed.[409]

However, according to the Ninth Circuit's recent holding, when criminal charges are filed, the government must provide some form of notice that evidence about a person was collected and is subject to surveillance.[410] This permits the defendant to determine whether the surveillance complied with the Fourth Amendment's requirements, "whatever the parameters of those requirements are."[411] However, the Ninth Circuit acknowledges that the need for secrecy in foreign intelligence investigations "justifies a more circumscribed notice requirement than in the ordinary criminal context."[412] The government is only required to provide notice, not disclosure because the disclosure of information to the defendant has the potential to harm national security interests.[413]

Conclusion

As Justice Brandeis notes in his dissent in *Olmstead v. United States*, "[Constitutions] are not ephemeral enactments, designed to meet passing occasions."[414] A two-pronged approach is required to protect our information. The court should adopt a comprehensive, narrowly tailored, and fluid approach to personal data. A legislative framework in regulating data is also required, public officials can navigate the complex nature of data privacy, without relying on the subjective *Katz* reasonable expectation of privacy framework. Relying on property-based considerations, legislatures have the opportunity to recognize and adapt the inherent rights guaranteed to personal data, and how these protections would apply.[415]

Citizens of the E.U. are increasingly using the GDPR and the privacy protections guaranteed under it.[416] Nevertheless, the effectiveness of the GDPR has been called into question many times.[417] The most important accomplishment of this statute is that it has changed the landscape of data

409. *Id.*

410. *Id.*

411. *Id.* at 1000.

412. *Id.*

413. *Id.* at 1001.

414. *Olmstead*, *supra* note 125, at 473.

415. *See generally* KERRY ET AL., *supra* note 3.

416. *Id.*

417. Rob Sobers, *A Year in the Life of the GDPR: Must-know Stats and Takeaways*, VARONIS (2020), https://www.varonis.com/blog/gdpr-effect-review/#enforcement.

privacy.[418] Although the enforcement is of the GDPR limited, it highlights the need for recognition and awareness of the protection of privacy. The developing awareness and concern about privacy rights online is a significant and growing global dilemma.[419] Nevertheless, there has been a significant lack of preparedness and difficulty for businesses and organizations to comply with these standards and European enforcement agencies are overwhelmed.[420]

As Congress prepares a comprehensive federal plan to address data privacy issues, it should pay attention to the significant implications of the court employing a legislative approach to recognize a property interest in personal data. The third-party doctrine, along with the *Katz* reasonable expectation of privacy framework provides a subjective test that is too broad for the court to apply.[421] Although the *Carpenter* decision is an example that addresses the potential implications, it employs the problematic *Katz* test that is difficult to apply, especially in the digital context.[422]

Individuals knowingly and voluntarily disclose their personal data to third parties daily.[423] Whether it's to a service provider or application, individuals provide almost all their information online.[424] Subjecting every form of online information to the reasonable expectation of privacy standard is both ineffective and unduly burdensome to the court.[425] A legislative effort to recognize personal data as an "effect" under the Fourth Amendment would permit the court to employ a more appropriate property-based trespass approach in conjunction with the court *Katz* reasonable expectation of privacy test, to properly assess an individual's right to privacy.[426] Furthermore, employing the 'mere evidence rule' appropriately limits the scope of searches of personal information to any "nexus" to a crime. Due to the limitless nature and scope of personally identifiable information online, there must be room to ensure protections against the government's broad reach.

By acknowledging property ownership of personal data, the judicial system can utilize the existing property and tort laws to determine and

418. *Id.*

419. *Id.*

420. *Id.*

421. *See* Harris, *supra* note 164, at 116-17.

422. *See* Margaret Hu, *supra* note 87, at 152-53 (2018).

423. Josephine Wolff, *Losing Our Fourth Amendment Data Protection*, N.Y. TIMES (Opinion) (2019), https://www.nytimes.com/2019/04/28/opinion/fourth-amendment-privacy.html.

424. *Id.*

425. *See* Brady, *supra* note 1, at 1017.

426. *See* Brady, *supra* note 1, at 1017; Harris, *supra* note 164, at 116-17.

allocate penalties for the abuse of sensitive information.[427] Such laws ensure the safety and future of society by preventing an unreasonable collection of private information by the government and by private entities without knowledge or consent. By allowing users to take ownership of their personal data, parties will reconsider the way they process and collect sensitive information. Personal data deserves protection because, in the current age, a person's most vital information is stored online. Without proper safeguards to discourage the manipulation of information, the future of privacy is in jeopardy.

The Schrems & *Moalin* decisions have placed U.S. Congress on notice, providing some encouragement to enact federal legislation on the issue. The European Union's GDPR and California's CCPA provide persuasive statutory frameworks to understand the potential implications of a federal data privacy regulation. Not only is it important for individuals to have these rights, but they should be aware of them. The potential consequences of unmonitored and unrestricted use of personal data are immense. Governmental abuse of power and unregulated collection and exploitation of personal data is likely an unavoidable consequence if no protections are implemented. While our information is continuously compiled, legislation must move forward to protect our constitutional privacy interest in data.

427. *See* Wolff, *supra* note 423.