THE DIGITAL PERSON: LAW ENFORCEMENT & THE PURCHASE OF DATA IN A POST-*CARPENTER* AGE

JAY E. TOWN*

* Jay Town is the former United States Attorney for the Northern District of Alabama and currently the Vice President and General Counsel at Gray Analytics. Prior to that, Town served as an Alabama State Prosecutor and a Judge Advocate in the United States Marine Corps, serving in each capacity for twelve years. Town earned his Bachelor of Arts degree from the University of Notre Dame in 1995 and graduated from Seton Hall Law School in 1998. Carpenter v. United States, 138 S. Ct. 2206 (2018); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (Geo. Wash. 2004). The "digital person" is truly a combination of "person" and "property" in the Fourth Amendment framework. The data involving the digital person tracks the human being and results in "papers" or "effects" transformed by the third-parties involved in the creation, maintenance, storage, or transfer of the data. The outward expressions and information shared by the digital person is the "digital voice." Therefore, it is not necessary to concede that digital data involves more than the person, but it is not dispositive either in the context of a search and seizure analysis.

INTRODUCTION

The Fourth Amendment is at an inflection point as courts adjust to a digital age. Born from *Carpenter v. United States*, the "digital person" is all the information that emits from our phones, tablets, devices, apps, and other personally identifiable effects that store a great deal of information about the end user. The *sound* of the digital person's voice comprises their geolocation, name, date of birth, physical address, IP address, purchase history, contact information, mobile phone number, and everything in between. The digital person leaves behind a trail of digital crumbs, which can then be devoured for various purposes.

One such purpose of utilizing this data is investigative. Basic data fusion can not only tell us where we are or what we are doing, but with whom we are doing it. As much as this reality may seem an encroachment on personal privacy, such was voluntarily sacrificed the moment an application was downloaded and terms and conditions agreed to. Data is streamed from the digital person voluntarily and collected for myriad purposes, including marketing, user improvement, and sales. Big Data[1]

1. "Big Data," discussed *infra,* describes multiple data sources that are collected regarding the digital person. Typically, Big Data refers to software, application, and device service providers who collect data provided voluntarily by users. The collection of the data is explained to, and agreed upon by, the user through the terms and conditions. For the purposes of this article, Big Data does not include Cell Site Location Information (CSLI) data since CSLI data is involuntarily conveyed. *See generally Big Data: 6 Unusual Ways*

market revenues are expected to eclipse $273 billion by 2026[2] and $655 billion by 2029.[3] The bulk of Big Data is collected by way of the privacy policies within the apps on our devices. So, whether you are checking the weather,[4] surfing social media,[5] or using a search engine[6] to find a privacy policy, it is likely that each application is tracking your digital person and sharing, marketing, or selling that information. And law enforcement is buying.[7]

Companies Can Collect Your Data, VILL. UNIV. (May 3, 2019), https://www.villanovau.com/resources/bi/6-ways-companies-can-collect-your-data/ [https://perma.cc/LZL4-G8TE].

2. *Big Data Market by Component, Deployment Mode, Organization Size, Business Function (Finance, Marketing & Sales), Industry Vertical (BFSI, Manufacturing, Healthcare & Life Sciences) and Region - Global Forecast to 2026*, MKTS. & MKTS., https://www.marketsandmarkets.com/Market-Reports/big-data-market-1068.html#:~:text=What%20is%20the%20projected%20market,11.0%25%20during%20the%20forecast%20period [https://perma.cc/FH6J-T2XA].

3. *Big Data Analytics Market Size, Share & COVID-19 Impact Analysis, By Component (Software, Hardware, and Services), By Enterprise Type (Large Enterprises, Small & Medium Enterprises (SMEs)), By Application (Data Discovery and Visualization, Advanced Analytics, and Others) By Vertical (BFSI, Automotive, Telecom/Media, Healthcare, Life Sciences, Retail, Energy & Utility, Government, and Others), and Regional Forecast, 2023-2030*, FORTUNE BUS. INSIGHT, https://www.fortunebusinessinsights.com/infographics/big-data-analytics-market-106179 [https://perma.cc/4KDA-LWT5].

4. The Weather Channel app, a seemingly innocuous application, has been downloaded millions of times. The app's privacy policy informs the user that his location information, or geolocation, will be collected along with other personal information (e.g., IP addresses, websites visited, etc.). The privacy policy also informs the user that users "have the ability to control how [their] data is used," including an ability to opt out of the app's tracking feature. If a user chooses not to opt out, his data will be shared with other websites, advertising vendors, and data bundling partners. *See Privacy Policy*, THE WEATHER CHANNEL (Jan. 1, 2023), https://weather.com/en-US/twc/privacy-policy#us-data-coll-tech-new [https://perma.cc/R7JG-VUHE].

5. Facebook is one of the most popular applications ever created. Its data policy informs users that Facebook collects, among many other data sets, "[d]evice locations, including specific geographic locations, such as through GPS, Bluetooth, or Wi-Fi signals," and "mobile phone number[s] and IP address[es]." *See Data Policy*, FACEBOOK (Sept. 29, 2016), https://www.facebook.com/about/privacy/previous#:~:text=We%20store%20data%20for%20as,to%20provide%20products%20and%20services [https://perma.cc/D6WZ-4ZFC].) The same Facebook data sharing policy informs users that Facebook, "transfer[s] information to vendors, service providers, and other partners."

6. Google is such a popular search engine in the United States that it is now a verb: "to Google." This app is auto-installed on both Google and Apple devices. Google's privacy policy informs users that it collects a host of personal information, such as IP addresses, mobile phone numbers, and geolocations of the user. The same policy tells users that they control what data is shared with Google, but otherwise that Google will otherwise share the data it receives with "publishers, advertisers, developers, or rights holders." Google also monetizes data by building individual profiles of users (with non-personally identifiable information) and then sells that data to advertisers and third-parties. *See Privacy Policy*, GOOGLE (Dec. 15, 2022), https://policies.google.com/privacy?hl=en-US [https://perma.cc/MAZ7-FTRG].

7. It has been widely reported that the Federal Bureau of Investigation, Department of Homeland Security, Department of Treasury, Internal Revenue Service, and Department of Defense have all purchased commercially available data related to the digital person. *See*

It once was reasonable to expect courts to rule that there is no reasonable expectation of privacy, even in the digital era, because nearly all of the information streamed from mobile devices, applications, and browsers is voluntarily shared per the terms of the platforms', websites', and applications' agreements. But then the United States Supreme Court issued its opinion in *Carpenter v. United States*.[8] Scholars and jurists alike opined, to some degree of hyperbole, on the enormity of the impact this holding would have on the Fourth Amendment going forward.[9] Defense counsel and privacy advocates regaled the case as a great win for privacy.[10] Prosecutors and law enforcement contemplated the impact on previous and future evidence gathering.[11]

But in the end, *Carpenter* was little more than an isolated enigma within the margins of search and seizure frameworks; the excitement around *Carpenter* was little more than a conflated flurry. Law enforcement can absolutely purchase digital person data and use it for investigative purposes without triggering the Fourth Amendment.

I. A BRIEF HISTORY OF THE FOURTH AMENDMENT

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" is the basic protection provided by the Fourth Amendment.[12] Our jurisprudence recognizes that the basic purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[13] Moreover, the interchangeability of "persons" and "digital person" is the inherent repercussion of *Carpenter*; the Fourth Amendment applies to both.

Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, BRENNAN CTR. FOR JUST. (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data [https://perma.cc/ZM8Q-HQ87].

8. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

9. *See, e.g.,* Matthew B. Kugler & Meredith Hurley, *Protecting Privacy Across the Public/Private Divide*, 72 FLA. L. REV. 451, 479–80 (2020); Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 385 (2019).

10. Ren LaForme, *The Supreme Court Just Struck a Major Victory for Digital Privacy*, POYNTER (June 25, 2018), https://www.poynter.org/tech-tools/2018/the-supreme-court-just-struck-a-major-victory-for-digital-privacy/ [https://perma.cc/YXC4-3BPD]; Michael Price & William Wolf, *Building on Carpenter: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider*, NAT'L ASS'N OF CRIM. DEF. LAWS. (Aug. 31, 2022), https://www.nacdl.org/Content/Building-on-Carpenter-Six-New-Fourth-Amendment-Cha [https://perma.cc/KYH6-P4C6].

11. *See generally* Ohm, *supra* note 9, at 390–92.

12. U.S. CONST. amend. IV.

13. *See Carpenter*, 138 S. Ct. at 2213 (quoting Camara v. Mun. Ct. of City and Cnty. of San Francisco, 387 U.S. 523, 528 (1967)).

A. The Birth of the Fourth Amendment

The Fourth Amendment itself was inspired by legal traditions and abuses that preceded the framing of the Bill of Rights.[14] "American Fourth Amendment jurisprudence was [originally] tied to common-law trespass."[15] The Amendment's birth can be traced back to 1762 Britain, where the King's messengers raided the home of John Entick, a writer critical of the Monarchy.[16] Entick promptly sued Nathan Carrington, the King's Chief Messenger, for trespass, and was victorious.[17] In the opinion of the Court of Common Pleas, Lord Camden, the Chief Justice, opined that "[t]he great end, for which entered into society, was to secure their property."[18] Lord Camden seemed to reference John Locke's *Two Treatises of Government*, which provided a similar analysis of private property and civil society nearly a century prior.[19] "The concept of security in property recognized by Locke and the English legal tradition appeared throughout the materials that inspired the Fourth Amendment."[20] The reviled writs of assistance[21] inspired the Revolution and became "the driving force behind the adoption of the [Fourth Amendment]."[22] John Adams was instrumental in drafting Article XIV of the Massachusetts Constitution, which "served as a model for the Fourth Amendment" and read, in part, that "[e]very subject has a right to be secure from all unreasonable searches and seizures of his person, his house, his papers, and all his possessions."[23] The idea that "the absolute rights of…all freemen, in or out of civil society, are principally personal security, personal liberty, and private property," is attributed to Adams in 1772, four years before the Declaration of Independence.[24]

B. The Early Fourth Amendment Cases

Many Supreme Court decisions have developed the search and seizure tapestry since our founding. In *Boyd v. United States*, the Supreme Court held that a federal law could not empower law enforcement to demand a citizen to produce papers or materials that would tend to

---

14. 3 WILLIAM BLACKSTONE, COMMENTARIES 288; JOHN LOCKE, TWO TREATISES OF GOVERNMENT (1690).

15. United States v. Jones, 565 U.S. 400, 405 (2012) (citing Kyllo v. United States, 533 U.S. 27, 31 (2001)).

16. Entick v. Carrington [1765] 95 Eng. Rep. 807, 807 (KB).

17. *Id.* at 818.

18. *Id.*

19. LOCKE, *supra* note 14, at 134.

20. Carpenter v. United States, 138 S. Ct. 2206, 2239 (2018) (Thomas, J., dissenting).

21. A "writ of assistance" is much like a search warrant, but has a requirement to actually find the object of the search. *See* Cooper v. Booth, 3 Esp. at 138; 170 Eng. Rep. at 565 (Lord Mansfield).

22. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990).

23. *Carpenter*, 138 S. Ct. at 2240 (Thomas, J., dissenting); MASS. CONST. art. XIV.

24. *See* SAMUEL ADAMS, THE RIGHTS OF COLONISTS 420 (Lib. of Cong. 1772).

incriminate him because such a law would be "repugnant to the Fourth and Fifth Amendments of the Constitution."[25] The Supreme Court began to refine its view of trespass by law enforcement in the context of the Fourth Amendment in *Hester v. United States*.[26] There, the Supreme Court ruled that even though law enforcement had trespassed on the defendant's property, there was no search of the "person" and therefore no illegal search.[27] Further refinement took place in *Olmstead*, where Chief Justice William Howard Taft delivered the opinion of the Court, opining that the Fourth Amendment was not violated when wiretaps were conducted without trespass.[28] However, the Supreme Court overturned *Olmstead* in *Katz v. United States,* ruling that a wiretap of a public phone violated the Fourth Amendment. Justice Harlan, in his famous concurring opinion, created what has since been referred to as the *Katz* Test.[29] This bifurcated test analyzes (1) whether the person had a subjective expectation of privacy in the place searched, and then (2) whether that expectation was objectively reasonable.[30] *Katz* signaled a shift from the traditional Fourth Amendment trespass or personal property analysis to a "reasonable expectation of privacy" framework.[31]

C. The Evolution of the Reasonable Expectation of Privacy Test

More contemporary opinions have employed the *Katz* test in various contexts of the Fourth Amendment. In *Miller*, the Supreme Court began the dogmatic creation of the "third-party doctrine," holding that the retrieval of a person's bank records without a search warrant was not in violation of the Fourth Amendment because a bank customer does not have a reasonable expectation of privacy in records kept by, and belonging to, a third-party bank.[32] The distinction drawn from the *Boyd* decision was that Boyd's papers were in his home, while the seized papers in *Miller* were held by a third-party bank.

The third-party doctrine grew stronger just three years later in *Smith v. Maryland,* wherein the Supreme Court held that the use and

25. Boyd v. United States, 116 U.S. 616, 621 (1886).

26. Hester v. United States, 265 U.S. 57, 59 (1924).

27. *Id*. It is important to understand that there can be no illegal seizure when there is no illegal search.

28. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

29. *See* Katz v. United States, 389 U.S. 347, 359 (1967).

30. *See id.* at 361 (Harlan, J., concurring). A person asserting a legitimate expression of privacy must have an actual, *subjective* expectation of privacy that is *objectively* reasonable.

31. *See* United States v. Jones, 565 U.S. 400, 405 (2012).

32. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442–43 (1976); Michael Gentithes, *The End of Miller's Time: How Sensitivity Can Categorize Third-Party Data after* Carpenter, 53 GA. L. REV.1039, 1042–43 (2019).

collection of pen registers[33] was not a search within the meaning of the Fourth Amendment.[34] Justice Blackmun's opinion in *Smith* applied the *Katz* test and determined that there was no objective or "legitimate expectation of privacy" regarding phone numbers dialed by a defendant to a third-party held in sum by yet another third-party.[35] The holding emphasized the "third-party doctrine," under which no person could have a legitimate expectation of privacy in information shared with a third party.[36]

D. Advancements in Technology & The Fourth Amendment

As new generations of technology were ushered into American lifestyles, new cases sparked new privacy analyses by the Supreme Court.[37] "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, [the Supreme Court] has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[38]

For instance, in *United States v. Jones*, a GPS[39] tracking device, without authority from a valid warrant, was put on the defendant's vehicle to monitor the vehicle's movements.[40] The Court ruled that affixing the GPS device to the vehicle was a search because the defendant's vehicle was among his personal "effects," and the government physically intruded upon that property for the purposes of a search.[41] This was perhaps the very first case involving the "digital person."[42]

In *Kyllo v. United States*, law enforcement used a thermal imaging device for surveillance. While there was no actual intrusion or trespass

---

33. "Pen registers" are little more than logs of incoming and outgoing phone calls made by a private party held as business records by the telephone service provider. *See Pen register*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/pen_register [https://perma.cc/XQE9-92VH].

34. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979); *see also* Rakas v. Illinois, 439 U.S. 128, 143–44 n.12 (1978) (admitting that "property concepts" are fundamental "in determining the presence or absence of the privacy interests protected by that Amendment").

35. *See Smith*, 442 U.S. at 743.

36. *Id.* at 744–45.

37. *See e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001).

38. *Id.* The Court held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search.

39. A "Global Positioning System" ("GPS") uses a satellite navigation system to provide the geographical location of the device – and to whatever it is affixed – at all times. *See What is GPS?*, NAT'L OCEAN SERV., (Jan. 20, 2023), https://oceanservice.noaa.gov/facts/gps.html [https://perma.cc/43H8-WVFD].

40. United States v. Jones, 565 U.S. 400, 405 (2012). It is important to understand that the Court in *Jones* did find that the placement of the GPS on the defendant's vehicle was a "search" in the context of the Fourth Amendment. However, the Court found that the defendant had no reasonable expectation of privacy in his whereabouts, or geolocation, on public streets in its *Katz* test analysis.

41. *Id.* at 404.

42. *See id.*

when using the device, the Court found this search violated the Fourth Amendment because citizens have an objective expectation of privacy inside their homes.[43] In *United States v. Karo*, the Supreme Court recognized that installing a "beeper" or tracking device on a third party's property before it was transferred to the defendant—and thus becoming part of the defendant's "personal effects"—was not a search or a seizure.[44] In *Riley v. California*, the Supreme Court recognized the "immense storage capacity" of personal cell phones; therefore, a search of the contents of a cell phone without consent or probable cause is an unconstitutional invasion of privacy.[45]

II. THE ARRIVAL OF *CARPENTER*

Carpenter v. United States entered constitutional scholarship with warm reception by some and discontent by others. Upon further review, the opinion is neither devastating to law enforcement nor the landmark case that some breathless privacy legal pundits made it to be. The holding is extremely important to understand in its entirety. It offers tremendous nuance and specificity in the context of the facts of the case. Furthermore, *Carpenter* emphatically notes its own limitations.

The key doctrinal language from the case, according to most scholars, is the following: "In light of the deeply revealing nature of [cell site location information], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third-party does not make it any less deserving of Fourth Amendment protection."[46] This one clause unceremoniously creates the "*Carpenter* factors."[47] *Carpenter* was considered by some to be the "end of the third-party doctrine" established by *Katz*, *Smith*, and *Miller*.[48] However, *Carpenter* does not have the impact on the Fourth Amendment that many of the scholarly articles immediately following its release suggested.[49] The opinion is more scalpel than blunt instrument.

---

43. Kyllo v. United States, 533 U.S. 27, 34 (2001).

44. *See* United States v. Karo, 468 U.S. 705, 712–13 (1984).

45. *See* Riley v. California, 573 U.S. 373, 403 (2014).

46. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

47. Lior Strahilevitz & Matthew Tokson, *Ten Thoughts on Today's Blockbuster Fourth Amendment Decision* Carpenter v. United States, CONCURRING OPS. (June 22, 2018), [https://perma.cc/Y94X-PTXR].

48. Orin S. Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT 37 (Oxford University Press 2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 [https://perma.cc/7RP7-URCY] (suggesting that the mosaic approach to privacy invasions in *Carpenter* created more confusion than it solved).

49. *See, e.g.*, Matthew Tokson, The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 135 Harv. L. Rev. 1790, 1800 (2022) (referring to the case as a "show-stopper [that] upsets the apple cart of the Fourth Amendment jurisprudence in a fundamental way").

A. Background of *Carpenter*

In *Carpenter*, a series of robberies took place in the City of Detroit in 2011.[50] A suspect confessed and identified a number of accomplices who participated in the robberies over a period of months.[51] By authority of the Stored Communications Act,[52] federal investigators subpoenaed cell site location information ("CSLI") for cell towers in the area of the robberies.[53] Carpenter's wireless carriers were compelled by subpoena, not bysearch warrant, and produced cell site data that ultimately led to Carpenter's conviction.[54]

Carpenter argued that a warrant, not other judicial process like a subpoena, was required to obtain the cell phone data under the Fourth Amendment.[55] The federal district court disagreed, and the Sixth Circuit affirmed that Carpenter "lacked a reasonable expectation of privacy in the [CSLI] collected by the FBI," since the cell phone records were business records belonging to the mobile phone service providers.[56] Carpenter appealed to the Supreme Court of the United States.[57] The Supreme Court sided with Carpenter, suppressed the CSLI, and reversed the conviction.[58]

B. The *Carpenter* Opinion

The *Carpenter* Court ran through the standard evaluation of *Katz* and its progeny as to what constitutes a search and a "reasonable expectation of privacy."[59] The Court explained that when "an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' [the Court has] held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[60] The Supreme Court continued with an analysis of the Fourth Amendment as it might pertain to emerging technologies and what may constitute a search, stating, "[a]s technology has enhanced the Government's capacity to encroach upon

50. *See Carpenter*, 138 S. Ct. at 2212.

51. *Id.*

52. *See* 18 U.S.C. §§ 2701–2703 (2018). An entire article could be written on the types of data that can be sold to law enforcement by application designers, software companies, and data collection third -parties. The sale of Big Data to law enforcement generally does not violate the Stored Communications Act or any current privacy law in the United States.

53. *See Carpenter*, 138 S. Ct. at 2212.

54. *Id.* at 2212–13.

55. *Id.* at 2212.

56. *Id.* at 2212–13.

57. Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016), *cert. granted.*, 85 U.S.L.W. 3567 (U.S. Jun. 5, 2017) (No. 16–402).

58. *See Carpenter*, 138 S. Ct. at 2223.

59. *Id.* at 2213–16.

60. *Id.* at 2213 (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).

areas normally guarded from inquisitive eyes, this Court has sought to 'assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[61] The *Carpenter* Court admonished that reasonable expectations of privacy cannot be "at the mercy of advancing technology."[62] The Court has explained that "advancing technology" includes thermal imaging devices,[63] GPS trackers,[64] cell phone storage capacity,[65] and now CSLI.[66]

However, the *Carpenter* Court also went to great lengths to affirm the third-party doctrine by acknowledging that "the Court has drawn a line between what a person keeps to himself and what he shares with others," which "remains true 'even if the information is revealed on the assumption that it will be used only for a limited purpose.'"[67] The opinion reaffirmed that "[a]s a result, the Government is typically free to obtain such [third-party] information from the recipient without triggering Fourth Amendment protections."[68] In other words, the government "typically" may still obtain third-party information without a warrant.

In the opinion's analysis of *Miller* and the third-party doctrine, the Court once again concluded that a person who can neither assert ownership nor possession of a record cannot sustain a legitimate expectation of privacy.[69] Moreover, the Court opined that certain records "to be used in commercial transactions" do not carry with them a reasonable privacy interest.[70] The analysis of *Smith* was similar in that the Court agreed that the use of a pen register was not a search.[71] The Court "doubted that people in general entertain any actual expectation of privacy in the numbers they

---

61. *See id.* at 2214 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001) (finding a thermal imaging device used to detect the defendant's home was a search and required a warrant for deployment)).

62. *See id.* (citing *Kyllo*, 533 U.S. at 35).

63. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

64. *See* United States v. Jones, 565 U.S. 400, 405 (2012).

65. *See* Riley v. California, 573 U.S. 373, 403 (2014).

66. *Carpenter*, 138 S. Ct. at 2206.

67. *Id.* at 2216 (citing United States v. Miller, 425 U.S. 435, 443 (1976)); *see also* United States v. Dionisio, 410 U.S. 1, 14 (1973) ("No person can have a reasonable expectation that others will not know the sound of his voice."); Donovan v. Lone Steer, Inc., 464 U.S. 408, 410–11 (payroll and sales records); California Bankers Assn. v. Shultz, 416 U.S. 21, 67 (1974) (Bank Secrecy Act reporting requirements); See v. Seattle, 387 U.S. 541, 544 (1967) (financial books and records); United States v. Powell, 379 U.S. 48, 49 (1964) (corporate tax records); McPhaul v. United States, 364 U.S. 372, 374 (1960) (books and records of an organization); United States v. Morton Salt Co., 338 U.S. 632, 651 (1950) (Federal Trade Commission reporting requirement); Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 189 (1946) (payroll records); Hale v. Henkel, 201 U.S. 43, 45, 75 (1906) (corporate books and papers).

68. *See Carpenter*, 138 S. Ct. at 2216.

69. *Id.* (emphasis added) (citing *Miller*, 425 U.S. at 443).

70. *Carpenter*, 138 S. Ct. at 2216 (reminding that the *Miller* Court concluded that an analysis of negotiable instruments (e.g., personal checks) could not carry with them a reasonable expectation of privacy).

71. *Id.*

dial" and recognized that subscribers know the data collected is used "for a variety of legitimate business purposes."[72] The *Carpenter* Court concluded its analysis in *Smith* by recognizing that defendant-Smith was voluntarily conveying information to a third party and "exposing that information . . . in the ordinary course of business."[73] Moreover, the *Carpenter* Court, in spite of its ultimate ruling, parroted the holding in *Smith* that defendants who voluntarily share information with third parties have "assumed the risk" that their data might be divulged to law enforcement.[74] This is compelling in that the voluntary nature of sharing information was not only recognized by previous opinions, but in *Carpenter* as well.[75]

However, the *Carpenter* Court ultimately concluded that the logic of *Smith* and *Miller* could not be extended to CSLI data.[76] The Court specifically held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements *as captured through CSLI*," and thus, the records gathered in *Carpenter* constituted a search requiring a warrant.[77] "A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] *seeks to preserve as private*, even in an area accessible to the public, may be constitutionally protected.'"[78] Chief Justice Roberts' opinion drew a comparison to *Jones* by noting, "[a]s with GPS information, the time-stamped [CSLI] data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations . . . [79] a cell phone [is] almost a 'feature of human anatomy.'"[80] In other words, a person has a reasonable expectation of privacy in his physical movements when *involuntarily* tracked through CSLI data.[81]

Regarding the voluntariness of disclosing otherwise private information, Chief Justice Roberts opined that "*Smith* and *Miller*, after all, did not rely solely on the act of sharing, but instead, they considered 'the nature of the particular documents sought'" to determine whether a reasonable expectation of privacy existed.[82] The opinion continues with a reminder that non-confidential communications used in commercial transactions are not cloaked with Fourth Amendment protections.[83] The opinion affirms the idea that "public movements" voluntarily conveyed to

72. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 742 (1979)).
73. *Id.* at 2216.
74. *Id.* at 2220.
75. *Id.*
76. *Id.*
77. *Id.* at 2217 (emphasis added).
78. *Id.* (citing Katz v. United States, 389 U.S. 347, 351–52 (1967)).
79. *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 415 (2012)).
80. *Id.* at 2218 (citing Riley v. California, 573 U.S. 373, 385 (2014)).
81. *Id.* (emphasis added).
82. *Id.* (citing United States v. Miller, 425 U.S. 435, 442 (1976)).
83. *Id.*

third parties do not travel with a reasonable expectation of privacy.[84] However, "more pervasive tracking" and "longer term" monitoring of involuntarily compiled data does constitute a search.[85] The CSLI in question in *Carpenter* contained "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[86]

However, Chief Justice Roberts' opinion pivots to the analysis of information that is "shared" with third parties.[87] The Chief Justice notes that "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user" and that "there is no way to avoid leaving behind a trail of location data."[88] Therefore, "in no meaningful sense does the user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements."[89] This is an incredibly important feature of this lengthy opinion, buried in a seemingly innocuous exchange about the pervasiveness of mobile phone utility.

Chief Justice Roberts then qualified the opinion in *Carpenter* by admonishing that:

> Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future."[90]

---

84. *Id.* at 2219–20 (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).

85. *Id.* (citing United States v. Jones, 565 U.S. 400, 430 (2012)). Note that the GPS device in *Jones* was placed on the vehicle by law enforcement, not collected by a third-party and given to law enforcement. The concept of the trespass to the Jones' vehicle played a starring role in the *Jones* opinion.

86. *Id.*

87. *Id.*

88. *Id.* It is important to note that the opinion recognizes how "indispensable" mobile phones are in American society because there is no real option in simply not possessing or carrying a mobile phone. Therefore, there is "no way to avoid leaving behind a trail of location data."

89. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 756 (1979)).

90. *Id.* at 2220.

Despite the Supreme Court ruling that the collection of CSLI was a search, and that a person has a reasonable expectation of privacy in the CSLI information collected, Chief Justice Roberts went to extraordinary lengths to limit the scope of the *Carpenter* decision, adamantly emphasizing the opinion is a "narrow one."[91] He admitted that the opinion "[leaves] open the question whether the warrant requirement applies 'when the Government obtains the modern-day equivalents of an individual's own papers or effects, even when those papers or effects are held by a third-party.'"[92] The holding carves out "real time CSLI and 'tower dumps.'"[93] Warrantless searches of CSLI are still permissible based on the "exigencies of the situation."[94] "Conventional surveillance techniques and tools" such as security cameras and perhaps pole-cams,[95] gunshot detection devices,[96] or other surreptitious surveillance techniques remain outside the scope of *Carpenter*.[97] The "opinion does not consider other collection techniques involving foreign affairs or national security."[98] The Court concludes by emphasizing the "*inescapable* and automatic nature of [CSLI data] collection" as a primary basis for the ruling.[99]

C. The *Carpenter* Factors

Carpenter was immediately scrutinized in various jurisprudential ways, often without prudence.[100] The opinion itself is altogether vague and

---

91. *Id.*

92. *Id.* at 2222 (citing United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010)).

93. *Id.* at 2220. "Tower dumps" are described by the Court as a download of information on all the devices that connected to a particular cell site during a particular interval.

94. *Id.* at 2222 (citing Kentucky v. King, 563 U.S. 452, 460 (2011)).

95. A pole camera, or "pole-cam," is a surveillance tool affixed to a structure, often a telephone or utility pole, which observes a certain location for some period of time. The surveillance itself is that which could be seen publicly, and the tool is meant to supplement law enforcement resources. In other words, the pole-cam replaces the need for human eyes to sit idle in the specific area for observation. These tools record what they surveil, which can be reviewed later. *See How Rapid Deployment Pole Cameras Benefit Law Enforcement*, WCCTV, https://www.wcctv.com/how-rapid-deployment-pole-cameras-benefit-law-enforcement/#:~:text=Pole%20Cameras%20allow%20for%20the,deterrent%20to%20deter%20potential%20offenders [https://perma.cc/U5RJ-ZKVK].

96. A "gunshot detection device," such as ShotSpotter™, employs analytical software and sophisticated acoustic sensors to detect and locate gunfire. These devices typically auto-alert authorities when the sensors detect a gunshot. *See ShotSpotter Frequently Asked Questions*, SHOTSPOTTER, https://www.shotspotter.com/system/content-uploads/SST_FAQ_January_2018.pdf [https://perma.cc/T7WY-XJSQ].

97. *See Carpenter*, 138 S. Ct. at 2220.

98. *Id.*

99. *Id.* at 2223 (emphasis added).

100. *See also* Aziz Huq, *The Latest Supreme Court Decision is Being Hailed as a Big Victory for Digital Privacy. It's Not.*, VOX, (Jun. 23, 2018, 7:43 AM), https://www.vox.com/the-big-idea/2018/6/22/17493632/carpenter-supreme-court-privacy-digital-cell-phone-

limited but does seem to carve out some specific factors that may inform courts going forward. Further, *Katz* was not overturned, nor was *Smith* or *Miller*.[101] If anything, the *Carpenter* case simply augments the primary framework of the *Katz test* with its own fact-specific factors.

Carpenter did not establish a litmus test for third-party data, nor did it dismantle the third-party doctrine or *Katz* test.[102] However, the opinion did establish a balance of critical factors that courts should consider when evaluating whether or not the retrieval of third-party data in any instance is a search, and whether defendants have a reasonable expectation of privacy in the data held by the third party.[103] In many ways, this is more in line with *Smith* and *Miller* than the breathless departure about which experts cautioned.

A single phrase in *Carpenter* may prove the most significant: "[i]n light of the deeply revealing nature of [CSLIn], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third-party does not make it any less deserving of Fourth Amendment protection."[104] From this one sentence, the *Carpenter* factors[105] can be established.

1. "Deeply Revealing Nature"

The "deeply revealing nature" of the information collected by the third party is a heightened category of the data collected regarding the private or digital person.[106] The Court in *Carpenter* found that the CSLI data in that case would provide a "detailed and comprehensive record of [a] person's movements."[107] The Court found that a "legitimate expectation of privacy" traveled with such a thorough and full tracking of personal whereabouts.[108] Therefore, deeply personal or private data may carry with it a reasonable expectation of privacy.[109]

But this is not dispositive.[110] First, not every retrieval of information is a search, regardless of expectations of privacy. Chief Justice

---

location-fourth-amendment [https://perma.cc/HD8T-ZPCR] ("It's not just that our digital privacy is insufficiently protected, in other words. It's that our Fourth Amendment rights and remedies in general have been eroded.").

101. *See* Matthew Tokson, *The* Carpenter *Test As A Transformation of Fourth Amendment Law*, 2023 U. ILL. L. REV. 507, 520 (2023); *see Carpenter*, 138 S. Ct. at 2220.

102. *See* Tokson, *supra* note 101, at 517.

103. *See* Tokson, *supra* note 49, at 1800.

104. *Carpenter*, 138 S. Ct. at 2223.

105. *See* Tokson, *supra* note 49, at 1801. Tokson's Article is an excellent examination of *Carpenter* and the "factors" that seemingly stemmed from that opinion. It is also an incredibly insightful review of search and seizure case law post-*Carpenter*.

106. *Id.*

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

108. *Id.*

109. *Id.*

110. *Id.*

Roberts went to great lengths to caution against any blanket rule as it relates to third-party data, simply refusing "to extend *Smith* and *Miller* to cover these *novel circumstances*" of CSLI third-party data.[111] The Court noted that CSLI is a "*qualitatively different* category of [third-party data]" and thus declined to apply *Smith* and *Miller* to the facts.[112]

This would further underscore that the type of data in *Carpenter* was itself "novel" to the Court, especially since seizure authority was derived from the Stored Communications Act.[113] Also, the "circumstances" of the retrieval of information were "novel" in that defendant-Carpenter had no control over the data shared with the third-party wireless carrier.[114] Moreover, the Court deemed the CSLI data to be "qualitatively different" from the data collected in *Smith*, *Miller*, and their progeny.[115] CSLI data was "unique"[116] and provided a "detailed chronicle of a person's physical presence" that "implicate[d] privacy concerns far beyond those considered in *Smith* and *Miller*."[117]

Deeply personal and private information about a person shared with a third party may carry with it a reasonable expectation of privacy.[118] The third-party doctrine cannot always be uniformly applied as a legal litmus test to digital technology and the digital person, primarily because the original opinions could not anticipate technological advancements.[119] The balance to the "deeply revealing nature" of a person—to include the digital person—is to "ensure that the 'progress of science' does not erode Fourth Amendment protections,"[120] while not having so broad an application as to "embarrass the future."[121] Thus, the application of *Carpenter* to the digital person is a narrow one, limited to the involuntary dissemination and collection of CSLI data.[122] Therefore, the "deeply revealing" CSLI data at issue in *Carpenter* is limited to "deeply revealing" data that is involuntarily revealed.

111. *Id.* (emphasis added).
112. *Id.* at 2216–17 (emphasis added).
113. *Id.* at 2212. There is some argument to be made that *Carpenter* was simply a rebuttal to the Stored Communications Act, in that the Act usurped the need for probable cause altogether. While not given analysis herein, it is clear throughout the dicta of *Carpenter* that the Court was unimpressed with the constitutional collision between the Fourth Amendment and the Stored Communications Act.
114. *Id.*
115. *Id.* at 2216–17.
116. *Id.* at 2220.
117. *Id.*
118. *Id.* at 2223.
119. *Id.*
120. *Id.* (citing Olmstead v. United States, 277 U.S. 438, 473–74 (1928)).
121. *See id.* (citing Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).
122. *Id.*

2. "Depth, Breadth, and Comprehensive Reach"

The Court's opinion further comments on the "depth, breadth, and comprehensive reach" of the CSLI data at issue in *Carpenter*.[123] The "reach" the Court describes is twofold.[124] First, the Court insists that mobile phones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[125] Second, CSLI is "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[126]

However, the Court qualifies the "depth, breadth, and comprehensive reach" of CSLI by stating unequivocally that the data shared through CSLI is "not truly shared as one normally understands the term."[127] The logical conclusion of such a distinction by the Court is that the data "shared" in *Carpenter* is different from data voluntarily conveyed to a third party.[128]

Data related to the digital person is purposefully shared by the user.[129] The terms and conditions set forth by Big Data inform the user that acceptance of those terms and conditions will reveal personal data that is comprehensive, personal, and extensive.[130] There is no doubt that Big Data seeks to collect data with "depth, breadth, and comprehensive reach,"[131] as it promises the user it will. The CSLI data analyzed in *Carpenter* is thereby easily distinguishable from Big Data and its depth, breadth, and comprehensive reach.

3. "Inescapable and Automatic Nature of Collection"

The *Carpenter* Court reasoned that cell phones are "almost a 'feature of human anatomy'"[132] and that the CSLI data born from cell phones is a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[133] CSLI data is collected by mobile phones "continuously scan[ning] their environment looking for the

123. *Id.* at 2223.
124. *Id.* at 2220.
125. *Id.* (citing Riley v. California, 573 U.S. 373, 385 (2014)).
126. *Id.*
127. *Id.*
128. *Id.* at 2219–20 (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).
129. *See* Ashley Stenning, *Gone But Not Forgotten: Recognizing the Right to Be Forgotten in the U.S. to Lessen the Impact of Data Breaches*, 18 SAN DIEGO INT'L L.J. 129, 130 (2016).
130. *Id.*
131. *See* Chad Squitieri, *Confronting Big Data: Applying The Confrontation Clause to Government Data Collection*, 101 VA. L. REV. 2011, 2031 (2015). Squitieri's analysis of Big Data, using Google as an example, describes the magnitude of data that Big Data collects.
132. *Carpenter*, 138 S. Ct. at 2218 (citing Riley v. California, 573 U.S. 373, 384 (2014)).
133. *Id.* at 2220.

best signal . . . several times a minute."[134] The data automatically collected indicates a general location, a time stamp, and has become "increasingly vast . . . and precise."[135] An expectation of privacy cannot be "at the mercy of advancing technology."[136]

The *Carpenter* Court disagreed with the opinion upholding the warrantless collection of CSLI data in which the Sixth Circuit declared that "cell phone users voluntarily convey cell-site data to their carriers."[137] Chief Justice Roberts' opinion declares that CSLI is "detailed, encyclopedic, and effortlessly compiled"[138] and recognizes that "what one seeks to preserve as private, even in an area accessible to the public, *may* be constitutionally protected."[139] Moreover, the *Carpenter* opinion recognized that individuals do not expect law enforcement to be able to track personal, private movements of the digital person for long periods of time.[140]

The expectation of privacy's constitutional protections, then, must be accompanied by the reasonableness of the expectation itself. Seeking to preserve information as private is a factor that may be protected by the Fourth Amendment.[141] Conversely, logic requires that information intended to be shared does not. Certainly, Facebook or ESPN applications are not "almost a 'feature of human anatomy,'" regardless of the amount of digital personal data chronicled daily.[142] Voluntary disclosure of otherwise private information to third parties carries with it no legitimate expectation of privacy in ordinary circumstances.[143] This is especially true when sharing the data involves an expectation that third parties will have access to the data, often for the conceived bargained-for benefit of the user.[144] Such data would not be considered "inescapable" or "automatic" since it is intentionally and preferably shared with Big Data.[145]

4. "Third-Party Possession"

It seemed an incredible departure from *Katz* when the *Carpenter* Court declared that "[t]he fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment

134. *Id.* at 2211.
135. *Id.* at 2211–12.
136. *Id.* at 2214 (citing Kyllo v. United States, 533 U.S. 27, 35 (2001)).
137. *Id.* at 2213.
138. *Id.* at 2216.
139. *Id.* at 2217 (citing Katz v. United States, 389 U.S. 347, 351-352 (1967)) (emphasis added).
140. *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (2012)).
141. *Id.* at 2217.
142. *Id.* at 2218 (citing Riley v. California, 573 U.S. 373, 384 (2014)).
143. *Id.* at 2216.
144. *See* Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 41 (2018) (demonstrating how users are more accepting of their lack of privacy when data collection is for their benefit).
145. *See id.*

protection."[146] *Carpenter* further held that the commercial purpose of the data "[does] not negate Carpenter's anticipation of privacy in his physical location."[147] The Court concluded that because Carpenter was unable to control or consent to data shared with the third-party service provider (namely CSLI data), Carpenter's expectation of privacy was reasonable.[148] The nature of the data shared, then, becomes important.[149] "*Smith* and *Miller*, after all, did not rely solely on the act of sharing. Instead, they considered "'the nature of the particular documents sought'" to determine whether there was a legitimate expectation of privacy in the contents of the data.[150] The Court's opinion distinguished *Miller* further by noting that the data in *Miller* did not consist of "confidential communications" but instead were intended for third-party use.[151]

There is no doubt that *Carpenter* proposes that a person may maintain a legitimate expectation of privacy in data or information held by a third party. What is also not in doubt is that data or information intended to be shared with the third parties for the benefit of the user is a critical factor in determining the existence of any reasonable expectation of privacy. There can be no "anticipation of privacy" when the user is requesting the data be shared with the third party. Regardless of the length of time the data is openly shared, or the sensitive nature of the data, if a person has no legitimate expectation of privacy there is no search or seizure.[152] As with automobiles,[153] egressing public areas,[154] or entering public commercial business,[155] a legitimate expectation of privacy diminishes when personal information, including a person's exact whereabouts at exact moments doing exact things, is voluntarily shared with third parties. Moreover, the user is seeking to share digital personal data expansively so that the utility of the app is also more expansive. The digital exhausts of the digital person are not only understood to be without privacy protections, but they are agreed upon by the party losing those protections.

5. Additional Carpenter *Factors*

Any analysis that fails to balance the aforementioned factors certainly fails to encompass the opinion in *Carpenter*. However, the Court in *Carpenter* did express interest in other minor factors worthy of

146. *Carpenter*, 138 S. Ct. at 2217.
147. *Id.*
148. *Id.* at 2224.
149. *Id.*
150. *Id.* at 2219 (citing United States v. Miller, 425 U.S. 435, 442 (1976)).
151. *Id.* at 2219.
152. *See generally* U.S. CONST. amend IV.
153. *See* Carroll v. United States, 267 U.S. 132, 149 (1925).
154. *See* Maryland v. Macon, 472 U.S. 463, 469 (1985).
155. *See* Donovan v. Dewey, 452 U.S. 594, 598–99 (1981).

discussion. The cost of the data to law enforcement, the number of persons surveilled in the collection of data, and the retrospective quality of the data have all been the subject of post-*Carpenter* decisions.[156]

There is no meaningful way to determine how persuasive these additional factors were or may be, but they were considered in a number of cases after *Carpenter* and worthy of note.[157] Typically, cost will be associated with the scale of surveillance, which will normally include a greater number of persons surveilled. Also, the ability of technology to discover the whereabouts of a person or persons retroactively, or track them continuously, has real privacy considerations.

D. Beyond *Carpenter*

The release of *Carpenter* sent shockwaves through the legal, academic, and law enforcement communities. With almost breathless punditry, legal scholars rushed to judge *Carpenter*'s impact on the third-party doctrine and search and seizure law. The hyperbole that accompanied the opinion was only matched by the outrage it caused to some. "*Carpenter* works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of constitutional privacy in this country for a generation or more."[158] Despite *Carpenter*'s missive that *Smith* and *Miller* were not disturbed in the decision, scholars deemed the ruling a "sharp break from prior third-party doctrine jurisprudence."[159] However, the lower courts have not interpreted *Carpenter* with the same inertia that permeated academic circles, and for good reason. *Carpenter* may have been limited to qualitative data sets, like CSLI, and thus does not neatly apply to other types of data or uses of it.

III. THE *CARPENTER* FACTORS V. "BIG DATA"

The term "Big Data"[160] has strained ontological roots, but generally describes multiple data sources "that are fast changing, large in both size and breadth of information, and come from [multiple] sources."[161] Moreover, Big Data is "collected passively as the digital exhausts of

156. *See* Tokson, *supra* note 49, at 1825. Tokson's informative analysis examines state and federal lower-level court decisions that analyzed *Carpenter*. Since none of these cases have been granted certiorari, no in-depth study was conducted here. However, the article by Tokson offers some interesting statistics on where the lower courts found footing with *Carpenter*.

157. *Id.*

158. *See* Ohm, *supra* note 9, at 358.

159. Kugler & Hurley, *supra* note 9, at 479–80, 496.

160. It is important to note that the data sources described herein as "Big Data" refer to data collected by third parties that is retrieved or sourced by the government, particularly law enforcement, without a search warrant or subpoena.

161. *Big Data*, U.S. CENSUS BUREAU (last updated July 7, 2022), https://www.census.gov/topics/research/big-data.html [https://perma.cc/QDS6-GRNZ].

personal and commercial activities."[162] Law enforcement can purchase Big Data without a warrant and without offending federal law or the Fourth Amendment.

In fact, many agencies within the United States Government use Big Data for mission oriented programming and services, including investigations.[163] The U.S. Census Bureau uses Big Data for "gathering more accurate information on the U.S. population and economy."[164] The Department of Defense employs Big Data for the detection of cyber espionage in military networks, among other things.[165] The Departments of Energy and Homeland Security use Big Data to improve the quality of their programs.[166] Federal law enforcement and intelligence agencies use commercial third-party data to enhance their predicated investigations and for investigative lead generation.[167] None of the data used by any of those departments was ingested or analyzed pursuant to a search warrant or subpoena.

It is also important to note that in the context of this analysis, the term "Big Data" does ***not*** include CSLI data. Big Data primarily refers to data that streams from the apps on a mobile phone or some other digital device and is collected by the app developer with the affirmative *voluntary* consent of the user. The use of the application or software in a given Big Data set is normally preceded by a series of permissions, privacy policy notifications, and even a certification that the user has read and agrees to the privacy policy.[168] This would include geolocation data of the user or digital person.

But what does the use of Big Data in a law enforcement context mean after *Carpenter*? It is not an open question. The Fourth Amendment analysis remains the same. Is the collection of Big Data a search? Is there a subjective expectation of privacy? Is it reasonable? At first glance, *Carpenter* seems to suggest that any vast data lake that tracks the

---

162. *Id.*

163. *See generally FBI Using Big Data To Predict Terrorism*, CYBER SEC. INTEL. (last updated Oct. 25, 2016), https://www.cybersecurityintelligence.com/blog/fbi-using-big-data-to-predict-terrorism--1783.html [https://perma.cc/UEX2-SNA9].

164. *Big Data*, *supra* note 161.

165. *See generally FACT SHEET: Big Data Across the Federal Government*, THE WHITE HOUSE (Mar. 29, 2012), https://obamawhitehouse.archives.gov/the-press-office/2015/12/04/fact-sheet-big-data-across-federal-government [https://perma.cc/W6FG-VQKK].

166. *Id.*

167. The commercial data referred to here, also known as AdTech or third-party data, includes geolocation data and social media scraping software.

168. Any website or application used on a device generally issues a request to accept the terms of the platform's privacy policy. Contained within those privacy policies is how an individual's data will be used, shared, or sold to third parties. While it is common for users to agree to the terms without reading through them, the terms are binding nonetheless. *See generally* Jessica Guynn, *What you need to know before clicking 'I agree' on that terms of service agreement or privacy policy*, USA TODAY (last updated Jan. 29, 2020, 2:21 PM), https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/ [https://perma.cc/3FNA-NBKM].

movement of individuals over long periods of time would offend the Fourth Amendment. However, a "*Carpenter* factors" analysis of the warrantless use of Big Data undoubtedly concludes otherwise.

A. The *Carpenter* Factors v. "Big Data": "Deeply Revealing Nature"

Big Data certainly carries with it a "detailed and comprehensive record of [a] person's movements,"[169] but there is no legitimate expectation of privacy in Big Data. Chief Justice Roberts went to great lengths to caution that the opinion in *Carpenter* covered the "novel circumstances" of CSLI. Moreover, *Smith* and *Miller* were not disturbed by the Carpenter decision. No blanketed rule was fashioned relating to third-party data, and the Court refused "to extend *Smith* and *Miller* to cover these *novel circumstances* [of CLSI third-party data]."[170] The Court noted that CSLI is a "*qualitatively different* category of [third-party data]" and thus declined the application of *Smith* and *Miller*.[171]

CSLI data is novel because there is nothing "voluntary" about the sharing or retrieval of it, except for the impractical solution of simply not using a mobile phone. Moreover, the authority for the subpoena for CSLI data in *Carpenter* was derived from the Stored Communications Act, further underscoring the specificity or novel circumstances "unique"[172] to CSLI data.[173]

The "deeply revealing nature" of a digital person, when voluntary, avoids the legal context and framework of *Carpenter* altogether. Voluntary disclosures of personal information to commercial third parties, which create in the aggregate Big Data has little distinction, if any, from the same person walking down the sidewalk in broad daylight screaming pitched admissions. Big Data does contain deeply revealing information, but the difference is that the digital person voluntarily shares the information. Many times, sharing is the point. Unlike CSLI data, the "progress of science" does not "erode Fourth Amendment protections" if the individual controls the information shared with third parties.[174] To determine otherwise would indeed "embarrass the future."[175]

---

169. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

170. *Id.* (emphasis added).

171. *Id.* at 2216–17 (emphasis added).

172. *Id.* at 2220.

173. *Id.* at 2212. There is some argument to be made that *Carpenter* was simply a rebuttal to the Stored Communications Act, in that the Act usurped the need for probable cause altogether. While not given analysis herein, it is clear throughout the dicta of Carpenter that the Court was unimpressed with the constitutional collision between the Fourth Amendment and the Act.

174. *Id.* at 2223 (citing Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)).

175. *Id.* at 2223 (citing Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

Under this *Carpenter* factor, no reasonable analysis would support a legitimate expectation of privacy or subsequent warrant requirement because the nature of the personal data revealed by the user of the application is intentional, calculated, and deliberate.[176] If the user never "seeks to preserve something as private," then any expectation of privacy is unreasonable.[177] Thus, official intrusions into that private sphere are not a search. If there is no search, there is no warrant requirement.

B. The *Carpenter* Factors v. "Big Data": "Depth, Breadth, and Comprehensive Reach"

Much like the deeply revealing nature of the data, Big Data has tremendous "depth, breadth, and comprehensive reach."[178] In fact, one could argue that is the point of Big Data: to share a location so that the user gets weather updates where they are currently located; to give personally identifiable information so that logins and purchases are a couple of convenient clicks on a device.; to have various utility in the discretion and participation of the user. For instance, one cannot reasonably argue that Facebook is "'such a pervasive and insistent part of daily life' [such that it could be considered] indispensable to participation in modern society."[179]

However, the geolocation data offered by Big Data sharing is absolutely "a detailed chronical of a person's physical presence compiled every day, every moment, over several years,"[180] even more so than CSLI.[181] But unlike CSLI, Big Data *is* "truly shared as one normally understands the term."[182] Big Data is "voluntarily conveyed" by the user to a third-party.[183] In fact, the user would find little or less utility and functionality in most applications if such distributions of personal information did not have such a comprehensive reach.[184] Because the *Carpenter* Court deliberately did not "disturb" the holdings in *Smith* and *Miller*, nor did it overturn their progeny such as *Knotts*, a digital person voluntarily providing personal data, is not significantly different than the relinquishment of legitimate expectations of privacy when driving an

176. *See* Barrett, *supra* note 144, at 41.
177. *Carpenter*, 138 S. Ct. at 2213.
178. *Id.* at 2223.
179. *Id.* at 2220 (citing Riley v. California, 573 U.S. 373, 384 (2014)).
180. *Id.* at 2220.
181. Margot E. Kaminski, Response, Carpenter v. United States: *Big Data Is Different*, GEO. WASH. L. REV. ON THE DOCKET (July 2, 2018), https://www.gwlr.org/carpenter-v-united-states-big-data-is-different/ [https://perma.cc/X46R-S7E2].
182. *Carpenter*, 138 S. Ct. at 2220 .
183. *Id.* at 2219–20 (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).
184. *See* Squitieri, *supra* note 131, at 2031.

automobile,[185] egressing public areas,[186] entering a public commercial business,[187] or purchasing goods from a third-party vendor.[188]

In *Knotts*, law enforcement placed a radio transmitter (or "beeper") in chemicals sold by a third party, which were to be used by the defendant in manufacturing illegal narcotics.[189] The officers followed the beeper for several days to the defendant's residence, where the narcotics were being manufactured.[190] The Supreme Court in *Knotts*, relying principally on *Smith*, held that the defendant had no "legitimate expectation of privacy [in the beeper he purchased] and thus there was neither a 'search' nor a 'seizure' with the contemplation of the Fourth Amendment."[191] In essence, the surveillance conducted by law enforcement in *Knotts* "amounted principally to the following of an automobile on public streets or highways."[192] The Court continued that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them."[193] The Court emphatically stated, "We have never equated police efficiency with unconstitutionality."[194] The Court even reasoned that law enforcement simply following the defendant after his purchase, with or without the beeper, would have resulted in the same discovery of the narcotics manufacturing site.[195] Despite the defendant being unaware of the tracking device, the Court ruled that he could have discovered the device any time by inspecting the contents of his purchase.[196]

Again, in *Carpenter*, the Court distinguished the long line of case law involving the dissemination of data or information to third parties based on the voluntary nature of the disclosure of that data.[197] Information gathered by law enforcement as a result of the actions of third parties does not offend the Fourth Amendment, nor do law enforcement activities that harness the enhancements of "science and technology."[198] Thus, it is clear in *Carpenter*'s holding that information that is voluntarily shared with, or gained by law enforcement through, a third party does not amount to a Fourth Amendment search or seizure, much less enjoy a legitimate

185. *See* Carroll v. United States, 267 U.S. 132 (1925).
186. *See* Maryland v. Macon, 472 U.S. 463 (1985).
187. *See* Donovan v. Dewey, 452 U.S. 594 (1981).
188. *See* United States v. Knotts, 460 U.S. 276 (1983).
189. *Id.* at 278–79.
190. *Id.*
191. *Id.*
192. *Id.* at 281.
193. *Id.* at 282.
194. *Id.* at 284.
195. *Id.* at 285.
196. *Id.* at 286–87 (Brennan, J., concurring).
197. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
198. *Knotts*, 460 U.S. at 282.

expectation of privacy.[199] The Court's refusal to disturb the third-party doctrine cases underscores the Court's differentiation between compulsorily shared data and data shared voluntarily. For those users of Big Data applications who fail or refuse to read the terms, conditions, or privacy policies provided to them, such failures cannot be attributed to law enforcement as violations of the Fourth Amendment.[200]

Based on this *Carpenter* factor, a reasonable analysis does not support a legitimate expectation of privacy or the need for a warrant, as the disclosing party intends and concedes to granting Big Data substantial "breadth, depth, and comprehensive reach."[201] Law enforcement can and should utilize technology, including Big Data, to enhance their investigative capabilities.[202]

C. The *Carpenter* Factors v. "Big Data": "Inescapable and Automatic Nature of Collection"

The *Carpenter* Court reasoned that cell phones are "almost a 'feature of human anatomy'"[203] and that the CSLI data born from cell phones are a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[204] But are phone applications? Is The Weather Channel app a "feature of human anatomy"? Is the use of Uber "inescapable"? Amazon? Twitter? In this context, sharing personal data may be compulsive, but is not compulsory.

The terms, conditions, and privacy policies presented to consumers and users by Big Data third-parties provide full notice to the user about disclosure, release, sharing, or sale of the same.[205] In the Big Data framework, an expectation of privacy is not "at the mercy of advancing technology."[206] Advancing technology is the root cause of the willing and voluntary disclosure of personal information to Big Data, even if that information would otherwise be subject to a legitimate expectation of privacy but for the intentional disclosure of it.[207] In fact, the voluntary

199. *Carpenter*, 138 S. Ct. at 2216.

200. *Knotts*, 460 U.S. at 286–87 (Brennan, J., concurring).

201. *See* Squitieri, *supra* note 131, at 2031.

202. *See generally FACT SHEET: Big Data Across the Federal Government*, *supra* note 165.

203. *Carpenter*, 138 S. Ct. at 2218 (citing Riley v. California, 573 U.S. 373, 385 (2014)).

204. *Id.* at 2220.

205. Przemysław Pałka & Marco Lippi, *Big Data Analytics, Online Terms of Service and Privacy Policies*, RSCH. HANDBOOK ON BIG DATA L. (forthcoming 2020) (manuscript at 1) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347364.

206. *Carpenter*, 138 S. Ct. at 2214 (citing Kyllo v. United States, 533 U.S. 27, 35 (2001)).

207. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFF. OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014) https://obama

disclosure of private data is often the purpose of the user's interface with the app. Therefore, the disclosure is clearly "escapable" and thus not "automatic" in its collection.[208] The user always controls the disclosures, is not seeking privacy, and can hardly be said to be "at the mercy" of Big Data.[209]

Under this *Carpenter* factor, no reasonable analysis would support a legitimate expectation of privacy or subsequent warrant requirement because the collection of the personal information is voluntary, intentional, and controlled entirely by the disclosing party.[210]

D. The *Carpenter* Factors v. "Big Data": "Third-Party Possession"

Carpenter signaled that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[211] The analysis does not conclude once data lands in other hands.[212] However, the Court's opinion also required that the communications with third parties be, at least in part, "confidential communications."[213] If such disclosures are meant for third-party use, intended to be shared, or are otherwise willingly provided to a third party for sale and marketing in the ordinary course of business, often to the benefit of the user, then no such legitimate expectations of privacy can exist.[214] As was the case in *Smith*, the defendant "voluntarily conveyed" the personal information and exposed that personal information for the third party to use in the ordinary course of business.[215] If a person has no legitimate expectation of privacy, there is no search or seizure.[216]

Big Data is third-party possession of personal data and does not implicate the Fourth Amendment.[217]

---

whitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/NH23-KDBB].

208. Chris Kirkham & Jeffery Dastin, *A look at the intimate details Amazon knows about us*, REUTERS (Nov. 19, 2021, 11:35 AM), https://www.reuters.com/technology/look-intimate-details-amazon-knows-about-us-2021-11-19/ [https://perma.cc/RR2Y-HC9B].

209. *Id.*

210. Pałka & Lippi, *supra* note 205, at 1.

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

212. *Id.*

213. *Id.* at 2216 (citing United States v. Miller, 425 U.S. 435, 442 (1976)).

214. *Id.* at 2216.

215. *Id.* (citing Smith v. Maryland, 442 U.S, 735, 744 (1979)).

216. *See generally* U.S. CONST. amend. IV.

217. *See* United States v. Morton Salt Co., 338 U.S. 632, 634, 651–53 (1950) (Federal Trade Commission reporting requirement); Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 189, 204–08 (1946) (payroll records); See v. Seattle, 387 U.S. 541, 544 (1967) (financial books and records); Hale v. Henkel, 201 U.S. 43, 45, 75 (1906) (corporate books and papers); United States v. Dionisio, 410 U.S. 1, 14 (1973) ("No person can have a reasonable expectation that others will not know the sound of his voice."); Cal. Bankers Ass'n. v. Shultz, 416 U.S. 21, 67 (1974) (Bank Secrecy Act reporting requirements); United States v. Powell, 379 U.S. 48, 49, 57 (1964) (corporate tax records); Donovan v. Lone Steer, Inc., 464

The *Carpenter* opinion clearly held that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[218] However, the crucial distinction drawn in *Carpenter* is the desire by the private party or user to share personal information with the third party, as opposed to "inescapable and automatic nature of its collection"[219] of it. Personal data is shared with third parties with the escapable, intentional detriment of the user.[220] There is no subjective expectation of privacy, much less a reasonable one.[221]

Under this *Carpenter* factor, no reasonable analysis would support a legitimate expectation of privacy or subsequent warrant requirement because the data is shared voluntarily with third parties and thus intended to be collected by third parties. As was the case in *Smith*, individuals "assume the risk" that third-party records will be "divulged to police" when such information is shared by the user voluntarily.[222]

E. The *Carpenter* Factors v. "Big Data": Additional Factors

The Court in *Carpenter* did note other minor factors that could be balanced against a mooting of reasonable expectations of privacy in Big Data. Data costs, quality, and scope should be considered by courts when applying *Carpenter*.[223] It is too soon to fully understand how courts will interpret these additional factors. However, it is compelling to note that the disclosing party benefits from the broadest possible scope of Big Data collection. The broader, the better. The more the data is shared across platforms and other applications, and the more data available to the third-party collector, the better the services provided to the private party discloser. Some apps track traffic patterns, which requires a massive sharing of real time geolocation data.[224] Some apps rate restaurants or entertainment venues, which the users of the application rely upon to make commercial purchase decisions.[225]

The scope of the data is intended to be broad.[226] The quality of the data is based on the scope.[227] And the cost of the data is normally based on

---

U.S. 408, 411, 415 (1984) (payroll and sales records); McPhaul v. United States, 364 U. S. 372, 374, 382 (1960) (books and records of an organization).

218. *Carpenter*, 138 S. Ct. at 2216.

219. *Id.* at 2223.

220. *See* Barrett, *supra* note 144, at 41.

221. *Id.*

222. *Carpenter*, 138 S. Ct. at 2216 (citing Smith v. Maryland, 442 U.S. 735, 745 (1979)).

223. *See* Strahilevitz & Tokson, *supra* note 47, at 1825.

224. Kirkham & Dastin, *supra* note 208.

225. *Fast Facts*, YELP (Mar. 31, 2023), https://www.yelp-press.com/company/fast-facts/default.aspx [https://perma.cc/9BWD-HRWZ].

226. *See* Squitieri, *supra* note 131, at 2031.

227. *Id.*

the breadth and quality of the data itself.[228] Therefore, the quantitative and qualitative nature of the data is intentionally expansive.[229]

Under these additional *Carpenter* factors, no reasonable analysis would support a legitimate expectation of privacy or subsequent warrant requirement because the purpose of interfacing with an application is often predicated by the third party ingesting large amounts of data. It is understood by way of the terms and conditions within the application that the user is voluntarily disclosing his private data for the non-exclusive benefit of the user.[230]

IV. THE SEARCH WARRANT REQUIREMENT EXCEPTIONS

This Article has exhaustively examined whether the purchase of Big Data is a search under the Fourth Amendment pursuant to *Carpenter*.[231] The conclusion drawn is that the purchase of Big Data by law enforcement for a law enforcement purpose is not a search, despite providing incredibly broad and specific information about individuals without a warrant.[232] However, it is feasible that a court could determine that the purchase of Big Data for warrantless use by law enforcement is a search.[233] In such a case, it would then be necessary to examine if the procurement of Big Data is a warrantless search without exception.

The definition of a *search* under the Fourth Amendment is not an elusive one.[234] A "search" occurs when an agent of the government violates an individual's reasonable expectation of privacy.[235] This "violation of privacy" is perfectly lawful in any number of circumstances, including when the search is conducted after a warrant has issued,[236] when proper consent is given to perform the search,[237] a search incident to an arrest,[238] exigent circumstances,[239] when evidence of unlawful conduct is in plain view,[240] or where national security or protection of the homeland are at

228. *Id.*
229. *Id.*
230. *See* Barrett, *supra* note 144, at 41.
231. *See supra* Section III.
232. *See infra* Conclusion.
233. The Court went to great lengths to preserve the holdings in *Katz* and its progeny, including *Smith* and *Miller*, while laying the foundation for legal debate over the future of the government use of data. Again, it is my contention that there is no legitimate right to privacy in Big Data.
234. Jule Pattison-Gordon, *Calls Mount for Blocking Warrantless Mass Data Collection*, GOV'T TECH. (July 20, 2022), https://www.govtech.com/public-safety/calls-mount-for-blocking-warrantless-mass-data-collection [https://perma.cc/UMY9-NPKW].
235. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).
236. U.S. CONST. amend. IV.
237. *See generally* Schneckloth v. Bustamonte, 412 U.S. 218 (1973).
238. *See generally* United States v. Robinson, 414 U.S. 218, 235 (1973).
239. *See generally* Missouri v. McNeely, 569 U.S. 141 (2013).
240. *See generally* Horton v. California, 496 U.S. 128 (1990)

stake.[241] "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."[242]

There are countless scenarios that the Court has determined a warrant is not required.[243] Law enforcement can fly over drug crops without it being a search.[244] Law enforcement can sift through a suspect's garbage without offending the Fourth Amendment.[245] Law enforcement can enter the property of a suspect outside of the curtilage of the home to observe criminal activity without a search warrant,[246] even if in the presence of a "no trespassing" sign.[247] Certainly law enforcement can approach a vehicle, and even detain the vehicle and passengers for a brief period of time, without a search warrant.[248] Even a legally defective search warrant relied upon in good faith by law enforcement does not violate the Fourth Amendment.[249]

If we entertain the premise that the purchase of Big Data by law enforcement is a search, it is laboriously necessary to examine the possible applicable exceptions to the warrant requirement.[250]

A. Consent to Search

The obvious starting point for an exception to the warrant requirement is a consent search.[251] It is well settled under the Fourth Amendment that a search conducted without a warrant is "per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions."[252] It is equally well settled that consent to search is an exception to the warrant and probable cause requirements of the Fourth Amendment.[253] Law enforcement has the burden of proving that the consent

241. Clapper v. Amnesty Int'l, USA, et al., 568 U.S. 398 (2013).

242. Riley v. California, 573 U.S. 373, 382 (2014). Note that there are other exceptions to the warrant requirement. Without a lawful exception, the exclusionary rule is the typical remedy. Under the exclusionary rule, any evidence connected to an unlawful search will be inadmissible in the Government's case-in-chief.

243. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

244. California v. Ciraolo, 476 U.S. 207, 213–14 (1986)

245. California v. Greenwood, 486 U.S. 35, 40–41 (1988)

246. United States v. Dunn, 480 U.S. 294 (1987).

247. Oliver v. United States, 466 U.S. 170 (1984).

248. Terry v. Ohio, 392 U.S. 1 (1968).

249. Arizona v. Evans, 514 U.S. 1 (1995). "[L]egally defective" means a warrant could have incorrect facts, data, record references, or even base the probable cause on a statute found later to be invalid. *See also* Herring v. United States, 129 S. Ct. 695, 704 (2009); Davis v. United States, 131 S. Ct. 2419, 2434 (2011).

250. Pattison-Gordon, *supra* note 234.

251. Fernandez v. California, 571 U.S. 291, 292 (2014).

252. Katz v. United States 389 U.S. 347, 357 (1967). It is important to note that the Fourteenth Amendment applies the Fourth Amendment requirements to state and local law enforcement activities.

253. Davis v. United States, 328 U.S. 582, 593–94 (1946).

was voluntary.[254] Voluntariness then becomes critical to the analysis, which is often difficult.[255]

There is "no talismanic definition of 'voluntariness' mechanically applicable to the host of situations where the question has arisen."[256] "It cannot be taken literally to mean a 'knowing' choice."[257] A person does not act voluntarily under the duress of violence[258] or when his will has been overborne.[259] Other factors that have been considered in determining voluntariness of incriminating evidence have included an accused's youth,[260] lack of education[261] or low intelligence,[262] and whether the accused was detained[263] or deprived of some necessity, such as food, water, or sleep.[264] "The problem of reconciling the recognized legitimacy of consent searches with the requirement that they be free from any aspect of official coercion cannot be resolved by any infallible touchstone."[265]

However, the "official coercion" discussed in *Schneckloth v. Bustamonte* does require some state action that is overbearing such that the consent was not truly voluntary.[266] In *Schneckloth*, the defendant was a passenger in a vehicle that was stopped by law enforcement.[267] The person in control of the vehicle gave consent to search, stolen checks were found linking back to the defendant, and the defendant was charged.[268] The defendant moved unsuccessfully to suppress the evidence found because the defendant had not given consent and the party that did not provide "knowledgeable consent".[269] In denying the motion to suppress, the Court ruled that "knowledge of the right to refuse consent is [not] a necessary prerequisite to demonstrating 'voluntary' consent."[270] The *Carpenter* Court opined that CSLI data sharing was not voluntary, making a right to refuse analysis impractical.[271] Moreover, the user is a "willing seller" of his or her

254. Bumper v. North Carolina, 391 U.S. 543, 548 (1968).
255. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).
256. Schneckloth v. Bustamonte, 412 U.S. 218 (1973).
257. *Id.* It has been widely reported that law enforcement purchases Big Data for law enforcement purposes. *See* Aaron Schaffer, *The FBI is spending millions on social media tracking software*, WASH. POST (Apr. 5, 2022 7:42 AM), https://www.washingtonpost.com/politics/2022/04/05/fbi-is-spending-millions-social-media-tracking-software/ [https://perma.cc/XGL9-PSCF].
258. Brown v. Mississippi, 297 U.S. 278 (1936).
259. Blackburn v. Alabama, 361 U.S. 199, 206–07 (1960).
260. Haley v. Ohio, 332 U.S. 596, 599–601 (1948).
261. Fikes v. Alabama, 352 U.S. 191, 196 (1957).
262. Payne v. Arkansas, 356 U.S. 560, 567 (1958).
263. *See* Chambers v. Florida, 309 U.S. 227, 239 (1940).
264. *See* Reck v. Pate, 367 U.S. 433, 441–42 (1961).
265. Schneckloth v. Bustamonte, 412 U.S. 218, 229 (1973).
266. *See id.*
267. *Id.* at 220–221.
268. *Id.*
269. *Id.* at 242.
270. *Id.* at 232–33.
271. *See generally* Carpenter v. United States, 138 S. Ct. 2206, 2216–20 (2018).

data in exchange for what is often free usage of an application.[272] When parties have mutual rights to a shared space or information, then either party may consent to a search.[273]

Certainly, the Fourth Amendment, per *Carpenter*, cannot now propose that consent must completely be understood and intelligently waived by every defendant.[274] To do so would eviscerate third party consent searches altogether.[275] Big Data retrieves the data at the behest of the user, with the user's consent that Big Data can do with that data as it will. When an application user accesses Big Data, the user does so voluntarily. The consumption of the data by the app provider is fully disclosed in the terms and conditions, and the user consents to those terms and conditions.[276] The user often wants to share personal information, such as geolocation data, for full functionality of the app by the user.[277] Therefore, this information is shared consensually by the user. Even if the collection by law enforcement of Big Data held by a third party constitutes a search, the warrant requirement is fully discarded by the user's consent.[278] After such consent there can be no legitimate expectation of privacy.

The consent exception to the warrant requirement is very similar to voluntary disclosure arguments, where there is no search at all to even trigger a Fourth Amendment analysis. But even if one was necessary, a *Carpenter* analysis could not support a legitimate expectation of privacy or subsequent warrant requirement because third parties have the user's consent.

B. Plain View

The plain view exception to the warrant requirement assumes there is legitimate expectation of privacy, and thus a search occurs.[279] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be

---

272. *See* Maryland v. Macon, 472 U.S. 463, 469 (1985). Here, the Court determined that law enforcement interfacing directly with a suspect by browsing that suspect's business, where all are free to browse, was not a search. A police purchase of magazines, though not a search, revealed unlawful conduct. The Court held that the defendant "voluntarily transferred any possessory interest he may have had in the magazines to the purchaser upon the receipt of the funds." *Id.*

273. United States v. Matlock, 415 U.S. 164, 170 (1974); s*ee* Illinois v. Rodriguez, 497 U.S. 177, 181 (1990).

274. *See Carpenter*, 138 S. Ct. at 2213–16.

275. Schneckloth v. Bustamonte, 412 U.S. 218, 245 (1973) (citing Coolidge v. New Hampshire, 403 U.S. 443, 487–90 (1971)).

276. *Privacy Policy*, *supra* note 4; *Data Policy*, *supra* note 5; Privacy Policy, *supra* note 6.

277. *Privacy Policy*, *supra* note 4.

278. *Id.*; *Data Policy*, *supra* note 5; *Privacy Policy*, *supra* note 6.

279. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

constitutionally protected."[280] Moreover, "a warrantless seizure by police of an item that comes within plain view during their lawful search of a private area may be reasonable under the Fourth Amendment."[281] Law enforcement must be in a lawful position to observe and access the incriminating evidence.[282]

In *Terry v. Ohio*, the Supreme Court acknowledged that the issue of "stop and frisk" encounters—which are commonplace law enforcement tactics today— had "never before been squarely presented" to the Court.[283] So as not to embarrass the future, the *Terry* Court recognized that "rapidly unfolding and often dangerous situations" create the "need of an escalating set of flexible responses" available to law enforcement.[284] The *Terry* Court declared that "[t]he exclusionary rule has its limitations, however, as a tool of judicial control. It cannot properly be invoked to exclude the products of legitimate police investigative techniques on the ground that much conduct which is closely similar involves unwarranted intrusions upon constitutional protections."[285]

The purchase of Big Data from third parties by law enforcement may be a digital frisk, but there is not even the "minor inconvenience and petty indignity" as in a *Terry* stop and frisk. Even if the purchase of Big Data is an unlawful search, a *Carpenter* analysis could not support a legitimate expectation of privacy or subsequent warrant requirement because the user has virtually disclosed the very same data to third parties in plain view.

C. Good Faith

The "good faith" exception can exist for the purchase of Big Data by law enforcement.[286] In fact, it is likely that future reviews by trial courts regarding the pre-*Carpenter* admissibility of CSLI data will be preserved and upheld by citation to the good faith exception.[287] It is even possible that law enforcement stockpiles data until the next "data source" is deemed to

280. *Id.* at 351–52.

281. Arizona v. Hicks, 480 U.S. 321, 323 (1987). It is important to note that much of the plain view doctrine case law offers analysis on whether there was a lawful search. The doctrine itself normally carries facts with it that suggest probable cause existed for the plain view seizure (e.g., narcotics or firearms in plain view during a search that was questionably lawful).

282. Horton v. California, 496 U.S. 128, 135–36 (1990).

283. Terry v. Ohio, 492 U.S. 1, 9–10 (1968). The "stop and frisk" paradigm involves no *seizure* in and of itself, but instead a stoppage of a person without probable cause and a search of their person. To frisk is to search.

284. *Id.* at 10.

285. *Id.* at 13.

286. *See, e.g.*, Davis v. United States, 564 U.S. 229, 238–39 (2011); Arizona v. Evans, 514 U.S. 1, 14 (1995).

287. *See Davis*, 564 U.S. at 238–39.

offend the Fourth Amendment, thereby bypassing the new holding in favor of the good faith exception.[288]

In *Arizona v. Evans*, law enforcement unknowingly relied upon an invalid search warrant.[289] In *Davis v. United States*, officers conducted a search based on binding precedent that was overturned after the search was conducted.[290] In *Herring v. United States*, administrative errors by law enforcement led to the discovery of criminal activity.[291] In each of these cases, and scores more, the Supreme Court ruled that law enforcement operating in good faith will exempt or otherwise cleanse the warrant requirement.[292]

The current landscape suggests that law enforcement can purchase Big Data. The *Carpenter* Court had the opportunity to limit these "intrusions" but chose not to do so. Moreover, law enforcement relies on Big Data, exercising apparent authority to possess and utilize the data for investigations.[293] Unless and until a court rules that such a practice violates the Fourth Amendment, the use of Big Data by law enforcement is conducted in good faith.[294]

Even if the purchase of Big Data constitutes an unlawful search, a *Carpenter* analysis could not support a warrant requirement because law enforcement presumably accesses Big Data in good faith.[295]

D. Exigency, National Security, and Border Searches

The analysis for the warrant exceptions of exigency, national security, and border searches are somewhat similar.[296] All involve the government's interest in protection of individuals.[297] All involve public

288. *What is a data lake?*, AMAZON, https://aws.amazon.com/big-data/datalakes-and-analytics/what-is-a-data-lake/ [https://perma.cc/7CQP-LVYD].

289. *See Evans*, 514 U.S. at 4.

290. *See Davis*, 564 U.S. at 235–36.

291. *See* Herring v. United States, 555 U.S. 135, 137–38 (2009).

292. *Id.* at 146–48; s*ee Evans*, 514 U.S. at 14–16; *see also Davis*, 564 U.S. at 240;.

293. Greg Ridgeway, *Policing in the Era of Big Data*, 1 ANN. REV. OF CRIMINOLOGY 401, 410 (2018).

294. *Compare* Carpenter v. United States, 138 S. Ct. 2206, 2222–23 (2018), *with Davis*, 564 U.S. at 238–39. This argument should have carried the day in *Carpenter* as well. Since *Carpenter*, many cases have allowed application of the good faith exception to the warrant requirement under a *Carpenter* framework. However, it is understood that this argument failed in *Carpenter*, weakening this exception to some extent.

295. *Compare Carpenter*, 138 S. Ct. at 2222–23, *with Davis*, 564 U.S. at 238–39.

296. Missouri v. McNeely, 569 U.S. 141, 148–49 (2013); Holder v. Humanitarian L. Project, 561 U.S. 1, 34–35 (2010); United States v. Ramsey, 431 U.S. 606, 616–18 (1977).

297. *Ramsey*, 431 U.S. at 616–18; s*ee McNeely*, 569 U.S. at 148–49; *see also Holder*, 561 U.S. at 34–35.

safety.[298] All involve actions by law enforcement where securing a warrant would be untimely and potentially dangerous.[299]

1. Exigency

An emergency situation can justify a warrantless search under certain circumstances.[300] Exigent circumstances exist when law enforcement has an objectively reasonable belief that a warrantless search is necessary (1) to render aid to an injured person or prevent injury to a person,[301] (2) when evidence of criminal conduct is being destroyed,[302] or (3) when law enforcement is in "hot pursuit" of an individual suspected of criminal activity.[303] For instance, in *Michigan v. Fisher*, the Supreme Court upheld an exigent search when officers had developed probable cause that the defendant had engaged in violent criminal activity.[304]

Law enforcement may have the need to access Big Data sets to identify individuals suspected of imminent criminal activity or the capture of a fugitive.[305] In such an instance, the government would need to be able to articulate the exigent need to access Big Data. Such articulation may unfortunately be necessary in the instance of an active shooter or potential mass casualty event. Exigency obviously applies to imminent threats to the homeland, either by domestic or foreign terrorist organizations.[306] Law enforcement may conduct warrantless searches of Big Data in these—and other—articulable exigent circumstances.[307]

2. National Security

National security is a necessary and valid exception to the warrant requirement. In fact, several laws have withstood judicial scrutiny in support of this exception.[308] For instance, the Foreign Intelligence Surveillance Act of 1978 (FISA)[309] justifies agents conducting surveillance

298. *Ramsey*, 431 U.S. at 616–18; s*ee McNeely*, 569 U.S. at 148–49; *see also Holder*, 561 U.S. at 34–35.

299. *Ramsey*, 431 U.S. at 616–18; s*ee McNeely*, 569 U.S. at 148–49; *see also Holder*, 561 U.S. at 34–35.

300. *McNeely*, 569 U.S. at 148–49.

301. *See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

302. *See* Kentucky v. King, 563 U.S. 452, 462 (2011).

303. *See* United States v. Santana, 427 U.S. 38, 42–43 (1976).

304. *See generally* Michigan v. Fisher, 558 U.S. 45 (2009).

305. Ridgeway, *supra* note 293, at 408–11.

306. *Santana*, 427 U.S. at 42–43; s*ee Stuart*, 547 U.S. at 403; *see also King*, 563 U.S. at 462.

307. *King*, 563 U.S. at 462; *Santana*, 427 U.S. at 42–43; s*ee* Missouri v. McNeely, 569 U.S. 141, 148–49 (2013); *see also* Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

308. Clapper v. Amnesty Int'l, USA, 568 U.S. 398, 402 (2013); Holder v. Humanitarian L. Project, 561 U.S. 1, 34–35 (2010).

309. FISA permits physical searches without a warrant from an Article III court. It is important to note that many scholarly articles have been written about FISA and its

of the digital person without a search warrant under the guise of national security.[310] FISA allows for the targeting of non-U.S. persons, groups, or entities located outside of the United States.[311] However, data collected from outside of the United States and transmitted to someone or a group within the United States can be lawfully intercepted in surveillance.[312] In 2021, there were 232,432 targets of observation under FISA by the intelligence community, which included the Federal Bureau of Investigation.[313] It was the judgment of our nation's intelligence apparatus that such was necessary under the guise of national security. The USA Patriot Act[314] and the USA Freedom Act[315] offer similar permissions for warrantless searches.

Justice Roberts made it clear in *Carpenter* that the "opinion d[id] not consider other collection techniques involving foreign affairs or national security."[316] *Carpenter* did not address any exceptions or the question of whether warrantless use of Big Data in a national security paradigm was inviolate of the Fourth Amendment.[317] The Court had every opportunity to do so, but expressly informed that it had not disturbed current investigative techniques.[318]

It stands to reason that national security concerns support an important, and unfortunately necessary, exception to the warrant requirement.[319] The laws of the United States support information gathering to protect the homeland.[320] Should warrantless information be gathered during these processes, and the processes followed correctly, such information can lawfully predicate criminal charges.[321] Much like the exigency analysis, the national security exception applies to Big Data in articulable circumstances.

---

implications on privacy and the Fourth Amendment. This article only recognizes exceptions to the warrant requirement and does not examine any of the fundamental controversies within Title 50 intelligence gathering. *See* 50 U.S.C. §§ 1801–1813.

310. *See id.* FISA was supplemented by the USA Patriot Act and the USA Freedom Act. Both these laws have been amended several times.

311. 50 U.S.C. § 1801.

312. *Id*. There are many procedures, not examined here, for data collection or surveillance of U.S. persons that must be statutorily followed by intelligence gathering officials.

313. *See* OFF. OF THE DIR. OF NAT'L INTEL., *Annual Statistical Transparency Report*, 17 (2022).

314. *See* 8 U.S.C. §§ 1701–1778.

315. *See* 50 U.S.C. §§ 1801–1813.

316. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

317. *See id.*

318. *See id.*

319. *See id.*

320. *See id.*

321. *See id.*

3. Border Searches

Searches of persons and effects that come into the United States have also been held to be an exception to the warrant requirement.[322] There is no legitimate expectation of privacy when crossing into the United States, especially if arriving unlawfully or if the search is of a vehicle crossing the border.[323] While a border search is a "search" as defined by Fourth Amendment case law, such warrantless searches are not "unreasonable" and do not violate the Fourth Amendment.[324] In fact, border searches permit the use of technology, without a warrant, to aid in the search.[325] Federal courts have even ruled that border searches "never require probable cause or a warrant."[326]

The *Carpenter* opinion did not disturb law enforcement deploying "other collection techniques involving foreign affairs," including law enforcement activities at our international borders and ports.[327] Border searches remain an exception to the warrant requirement.[328] If the use of Big Data were to aid law enforcement in stopping, frisking, searching, or otherwise detaining individuals at the border, doing so would not offend the Fourth Amendment because of the highly diminished legitimate expectation of privacy one has at the border.[329]

Much like the exigency and national security analyses, border searches are a legitimate exercise of discretion that do not require a warrant.[330] The United States protects its borders, and those within the country, without triggering the Fourth Amendment.[331] In an instance where Big Data informs law enforcement for the purpose of protecting America's borders, such data collection and consumption would not collide with the Constitution.

CONCLUSION

Big Data is collected on the digital person everywhere. It is invasive. It is inclusive. But it is not involuntary. The collection of Big Data by software companies, service providers, and the like occurs only with the express consent of the user. Users get more from apps when their digital

322. Almeida-Sanchez v. United States, 413 U.S. 266, 272–73 (1973); United States v. Ramsey, 431 U.S. 606, 616–18 (1977); United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004); *see also* Carroll v. United States, 267 U.S. 132, 153–54 (1925).

323. Almeida-Sanchez, 413 U.S. at 272–73; Flores-Montano, 541 U.S. at 152–53; *see* Carroll, 267 U.S. at 153–154; s*ee also Ramsey*, 431 U.S. at 616–18..

324. *See Almeida-Sanchez*, 413 U.S. at 272–73.

325. *See* United States v. Vergara, 884 F.3d 1309, 1312 (11th Cir. 2018).

326. *Id.* (citing *Ramsey*, 431 U.S. at 619).

327. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

328. *See Vergara*, 884 F.3d at 1312.

329. *See id.*

330. *See id.*

331. *See id.*

person is shared, when the sound of their digital voice is shared, and when their geolocation is shared. Search terms are revealed, and posts are consumed by other users. Big Data collects invaluable information from the user and makes it cognizable for sale.[332] The sale could be for marketing, research, or customer service improvements.[333] But the sale could also be for use by law enforcement.[334]

In this context, law enforcement is not "buying their way around" the Fourth Amendment. Such a pejorative and ad hominem expression lacks any honest analysis of Fourth Amendment jurisprudence. Rather, law enforcement is enhancing its existing sensory faculties with the very technology citizens ask it to police.[335] Law enforcement should make no apology for supplementing its sensory faculties with information that is true and accurate, like Big Data.[336] The Fourth Amendment simply is not implicated because the digital person is not searched.[337] The digital person voluntarily exposes all the data collected with knowledge that third-parties, to include law enforcement, may take a peek. These voluntary disclosures, by way of terms and conditions for use, strip any subjective or legitimate expectations of privacy for the digital person.[338] The absence of a search allows law enforcement to access Big Data without a warrant.[339] The digital person exists in a digital world. It is beyond ridiculous that law enforcement should commit to living in an analog one.

The *Carpenter* factors establish that the use of Big Data by law enforcement does not collide with the Fourth Amendment.[340] Big Data is deeply revealing, with comprehensive reach and depth.[341] Big Data is collected automatically. But the *Carpenter* factors also recognize that what is revealed is done so voluntarily, that Big Data's reach and depth is at the discretion of the user, and that the automatic nature of the data collection is not inescapable.[342]

---

332. *Privacy Policy*, *supra* note 4.

333. *Privacy Policy*, *supra* note 4.

334. *See Privacy Policy*, *supra* note 4; *see also Privacy Policy*, *supra* note 6.

335. It is irrelevant whether law enforcement chooses to input Big Data into algorithms or artificial intelligence tools or continues with traditional "gum shoe" reviews of information. Access to the data is all that is pertinent to a *Carpenter* analysis. *See* Ridgeway, *supra* note 293, at 404–05.

336. *See id.* at 405.

337. *See Privacy Policy*, *supra* note 4; *see also Data Policy*, *supra* note 5; Privacy Policy, *supra* note 6.

338. *Privacy Policy*, *supra* note 4; *Data Policy*, *supra* note 5; *Privacy Policy*, *supra* note 6.

339. *See Privacy Policy*, *supra* note 4; *see also Data Policy*, *supra* note 5; *Privacy Policy*, *supra* note 6.

340. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217–19 (2018).

341. Ridgeway, *supra* note 293, at 402–06.

342. *See Carpenter*, 138 S. Ct. at 2217–19.

The digital age has transformed every aspect of the American lifestyle.[343] The way we communicate, educate, work, perform services, travel, dine, shop, and otherwise consume goods and services has completely changed in the last two decades.[344] The digital person's activities are more in "plain view" than ever before.[345] To be certain, the Fourth Amendment "protects people, not places."[346] So, there is a natural tension between the Fourth Amendment and the digital person, in that the digital person shares information with third parties to enhance the digital experience. While people may subjectively believe that there is a legitimate expectation of privacy in their browser history or app inputs, the legal reality is traversing the internet of things is no different than a virtual stroll down a crowded thoroughfare in broad daylight.[347] A conclusion otherwise would most certainly "embarrass the future," deny the reality of digital global behavior, and cannot be an expectation of privacy in which "society is prepared to recognize as reasonable."[348]

Justice should take caution that it "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[349] Law enforcement should be encouraged to use Big Data for predictive leads and predicated investigations alike. We have created these public squares for the digital person, and law enforcement is not obviating the Constitution by enhancing their sensory faculties with technology. There is no violation of the Fourth Amendment when law enforcement accesses voluntarily disclosed information from the digital person. To conclude otherwise would not only embarrass the future but punish it as well.

A person cannot expect the government to not know the sound of his voice, even if that voice is digital.

---

343. *See* Robert Kormoczi, *What is the Digital Age?*, TIMES INT'L (June 24, 2020), https://timesinternational.net/the-digital-age/ [https://perma.cc/SVZ5-K8PM].

344. *See id.*

345. *See supra* Section IV.B.

346. *See Carpenter*, 138 S. Ct. at 2217–19 (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

347. It is understandable that users of applications and the internet would prefer that their search history or sites visited were not broadcast to the world. However, such expectations of privacy cannot be any more legitimate than a person wanting the sound of his voice protected or wanting no one to look at him while walking down a busy street. A user cannot agree to share his personal, and otherwise private, information or thoughts with untold numbers of third-parties and then reasonably expect such information to be protected by the Fourth Amendment. *See Privacy Policy*, *supra* note 4; *Data Policy*, *supra* note 5; *Privacy Policy*, *supra* note 6.

348. Smith v. Maryland, 442 U.S. 735, 740 (1979).

349. *Carpenter*, 138 S. Ct. at 2233 (Kennedy, J., dissenting) (citing Ontario v. Quon, 560 U.S. 746, 759 (2010)).