OF CLOUDS AND CLOCKS: POLICE LOCATION TRACKING IN THE DIGITAL AGE

Steven I. Friedland[*]

* Professor of Law, Elon University School of Law. J.S.D., Columbia University, 1999; LL.M., Columbia University, 1994; J.D., Harvard Law School, 1981; B.A., State University of New York at Binghamton, 1978.

I. INTRODUCTION

Government authorities have tracked suspects for centuries.[1] In pre-electronic times, tracking generally was physical and often required significant police resources to follow the path of suspects.[2] Sometimes, the suspect evaded police; at other times, the police successfully captured the suspect.[3] Because of the resources required, tracking usually did not occur without some justification, at least for any sustained length of time.[4] Instead, it often occurred as part of an existing criminal investigation.[5] While secrecy was an integral component of tracking strategy, tracking was susceptible to detection and the experience of surveillance.[6]

Times have changed. Today, we live in a world of multiple mass surveillance systems, from drones to Internet information interceptors to face recognition software and more.[7] The government, private companies, and individuals all operate these surveillance systems.[8] More than 100,000 people employed by the National Security Agency (NSA) operate many programs,[9] from bulk telephone number collection[10] to the tracking of international–U.S. communications.[11] Numerous companies, such as Google and Amazon, gather users' data, aggregating and analyzing the data through

---

1. *See* Catherine McNiff, *Timeline: US Spying and Surveillance*, INFOPLEASE, http://www.infoplease.com/us/government/spying-surveillance-timeline.html (last visited Sept. 23, 2015).

2. *See* Jordan Miller, *New Age Tracking Technologies in the Post*-United States v. Jones *Environment: The Need for Model Legislation*, 48 CREIGHTON L. REV. 553, 558 (2015) (noting that 1980s beeper technology required the police to consistently follow a beeper's signal, which prevented the beeper "from replacing the physical presence of in-the-field officers when conducting investigations").

3. *See* United States v. Knotts, 460 U.S. 276, 278 (1983). For example, in *Knotts*, a case in which a beeper was installed to assist in tracking some individuals thought to be engaged in a drug operation, the physical police tail lost the car being followed; it was only a helicopter tracking the beeper that allowed the police to pick up the trail of the perpetrators once again. *Id.*

4 Miller, *supra* note 2, at 559 (noting that the significant costs and limitations of the early beeper technology limited its use to only necessary situations in which police had probable cause and a high chance of detecting criminal activity).

5. *Id.*

6. *See* Eva Marie Dowdell, Comment, *You Are Here!–Mapping the Boundaries of the Fourth Amendment with GPS Tracking*, 32 RUTGERS COMPUTER & TECH. L.J. 109, 117 (2005) (maintaining that early police tailing of suspects was riskier than modern GPS technology).

7. *See generally* Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281 (discussing various modern-day mass surveillance technologies).

8. *See id.* at 289 (discussing the exchange of personal data, obtained by private companies through surveillance, between private organizations and the government for the purposes of criminal investigations).

9. *See* Ewen MacAskill, Julian Borger & Glenn Greenwald, *The National Security Agency: Surveillance Giant with Eyes on America*, GUARDIAN (June 6, 2013, 6:55 PM), http://www.theguardian.com/world/2013/jun/06/national-security-agency-surveillance.

10. *See* G. Michael Fenner, *Edward Snowden: Hero or Traitor?*, MONT. LAW., Dec. 2014–Jan. 2015, at 16.

11. *See* Lothar Determann & Karl T. Guttenberg, *On War and Peace in Cyberspace: Security, Privacy, Jurisdiction*, 41 HASTINGS CONST. L.Q. 875, 876 (2014).

computer algorithms.[12] Individuals track themselves in different ways, from the carrying of a cell phone,[13] to the use of other smart things connected to the Internet, such as the devices offered by Fitbit, which self-describe as tracking a person's everyday health and fitness.[14]

These unassuming mass surveillance systems generally use "Big Data" sorting mechanisms as a tool to efficiently track persons around the clock and preserve information in perpetuity.[15] Big Data can analyze and recombine the information through complex algorithms to yield additional data.[16] The digital systems are often invisible and of little cost to the trackers.[17] Those tracked are rarely exposed to the experience of tracking. In fact, invisibility makes tracking seem to disappear, reducing its harm, especially when the tracking occurs in public places.[18] The government and private companies can track people remotely and at relatively little cost.[19]

The digital era has changed the underpinnings of assumptions about police tracking to such an extent that the rules of the Fourth Amendment relating to police tracking, and searches in general, are outdated. As Justice Sotomayor noted in her concurrence in *United States v. Jones*,[20]

> I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance."[21]

The question for today, then, is whether sufficiently predictable lines can be drawn to limit police tracking in the rapidly diminishing private

---

12. *See* Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 437 (2014) (referring to Google's privacy policy and Amazon's privacy notice).

13. *See, e.g.*, State v. Earls, 70 A.3d 630, 631–33 (N.J. 2013) ("With increasing accuracy, cell phones can now trace our daily movements and disclose not only where individuals are located at a point in time but also which shops, doctors, religious services, and political events they go to, and with whom they choose to associate.").

14. *See Fitbit.com Privacy Policy*, FITBIT, http://www.fitbit.com/privacy (last updated Dec. 9, 2014).

15. *See* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 384–87 (2010).

16. *See* Joshua A. T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1009 (2014) (discussing the role of Big Data in the aggregation of additional data).

17. *See generally* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000) (exploring various tracking technologies and surveillance systems, their availability to the government and private sector, and their transparent effect on the lives of average citizens).

18. *See id.* at 1468–71.

19. *Id.* at 1463 ("[B]oth the state and the private sector now enjoy unprecedented abilities to collect personal data, and . . . technological developments suggest that costs of data collection and surveillance will decrease, while the quantity and quality of data will increase.").

20. *See* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

21. *Id.* at 956 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

domain. This is particularly an issue with tracking in public through a satellite-based monitor (SBM), a global positioning system (GPS), or disclosures of information to third parties.[22]

At first glance, it is tempting to conclude there is no privacy from police tracking in public. This is especially true given the *United States v. Miller*[23] and *Smith v. Maryland*[24] line of cases, collectively known as the third-party doctrine, where information voluntarily disclosed to third parties is no longer private. Add to the mix face recognition software, Big Data, and private company tracking, and it would appear even more obvious that there are no limits to tracking in public under the Fourth Amendment. It is also tempting to enforce older, seemingly predictable bright lines like the trespass test of *Olmstead v. United States* to show continuity.[25] Yet, going back in time just to preserve a bright-line rule is not the answer.

A structure that can make sense of these issues exists, though. It originates outside of the Fourth Amendment domain. The protocol emanates from the domain of philosophy. The philosopher, Karl Popper, framed the difference between "clouds and clocks," and unknowingly illustrated how digital era police tracking can be aligned with the design of the Fourth Amendment.[26] Professor Popper wrote about clouds and clocks in the context of resolving the problem of rationality and the freedom of humans to choose.[27] To Popper, clouds represented physical systems that were "highly irregular, disorderly, and more or less unpredictable," like gases or a cloud of gnats.[28] Clocks, on the other hand, presented the opposite extreme, representing physical determinism, "physical systems which are regular, orderly, and highly predictable in their behavior."[29] On the issue of whether humans were clocks or clouds, Popper opted for clouds, saying humans are not automatons or mere computing machines.[30] Humans and other organisms are a hierarchical system of clouds controlled by clouds, with partial control

---

22. *See* Derek P. Richmond, *Can You Find Me Now?–Tracking the Limits on Government Access to Cellular GPS Location Data*, 16 COMMLAW CONSPECTUS J. COMMS. L. & TECH. POL'Y 283, 284 (2007).

23. *See* United States v. Miller, 425 U.S. 435, 444–45 (1976), *superseded by statute*, Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified as amended at 12 U.S.C. § 3401 (2010)), *as recognized in* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) (holding the respondent did not possess a valid Fourth Amendment interest to challenge a subpoena because information disclosed by a third-party bank did not violate his Fourth Amendment rights).

24. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the "petitioner . . . entertained no actual expectation of privacy in the phone numbers he dialed . . . and use of a pen register, consequently, was not a 'search,' and no warrant was required").

25. *See, e.g.*, *Jones*, 132 S. Ct. at 950 (majority opinion) (relying on the *Olmstead* physical trespass test to ground the decision, rather than a test responsive to the new era of technology).

26. *See* KARL POPPER, *Of Clouds and Clocks*, *in* OBJECTIVE KNOWLEDGE: AN EVOLUTIONARY APPROACH, 206–55 (Oxford Univ. Press rev. ed. 1979).

27. *Id.*

28. *Id.* at 207.

29. *Id.*

30. *Id.* at 222–26.

and partial suppression being exerted by the controlling clouds.[31] The cloud controls lie between pure chance and complete determinism.[32] The physical world is thus an open system of evolution characterized by trial and error.[33]

In light of this framework, the Fourth Amendment should be seen as creating a set of flexible cloud controls over police access to information. Using Professor Popper's thesis, this Article suggests that the flexible controls of a revised third-party rule and a mosaic theory of limits are consistent with the Framers' revulsion against unrestrained and unchecked police activity, as exemplified by general warrants.[34]

While the police can and will access a wide variety of information, there must be boundaries.[35] The private sphere must still be respected and protected under the Fourth Amendment, and while the center of gravity has rotated away from the physical house to such things as password protected information relayed to third-party institutions, the new electronic center of gravity should still be protected.[36] Because we have become a society that expects private companies to obtain and store buckets of personal information (although the American consumer does not like it), this expectation permits the government to obtain this information and circumvent the spirit of the Fourth Amendment.[37] Because the opening or closing of a door or window is not the same thing in the digital world as compared to the pre-digital world, the "plastic controls" fashioned by courts under the Fourth Amendment ought to be tailored to this new world ordering.[38]

It is the thesis of this Article that Fourth Amendment privacy represents a cloud problem, one the Justices of the Supreme Court have not yet properly tackled.[39] The Amendment is of diminished value if the Supreme Court still uses physical spatial dimensions, with all its clock-like regularity, to limit cyber-surveillance.[40] Further, the use of Big Data to aggregate and analyze data looks like it transforms people from clouds to clocks, but in reality, it does not.[41] Big Data just skews how privacy exists, but should not be allowed to effectively eliminate it.

---

31. *Id.* at 245.
32. *Id.* at 248–50.
33. *Id.* at 241–44.
34. *See infra* Part III.
35. *See infra* Part III.A.
36. *See* United States v. Jones, 132 S. Ct. 945, 949–53 (2012) (explaining that government tracking of electronic signals can constitute a Fourth Amendment search).
37. *See* Natasha Singer, *Sharing Data, But Not Happily*, N.Y. TIMES (June 4, 2015), http://www.nytimes.com/2015/06/05/technology/consumers-conflicted-over-data-mining-policies-report-finds.html?_r=0.
38. *See* POPPER, *supra* note 26, at 240; *infra* Part II.B.
39. *See infra* Part II.C.
40. *See infra* Part II.C.
41. *See infra* note 131 and accompanying text.

This Article instead suggests that the mosaic theory advanced in Justice Sotomayor's and Justice Alito's concurrences in *Jones* can limit the scope and extent of police tracking.[42] The mosaic theory, which contends that the aggregation of data from government cyber-surveillance can go "too far" and become a search, even when the unaggregated individual pieces of data do not, ought to be adopted as a flexible cloud control by the Court.[43] At some point, the spigots of information flowing to the Executive Branch of the government need to be monitored and even turned off to preserve two relationships—the first between the government and the people, and the second between the Executive and other branches.[44] This is especially important with respect to a particularly nettlesome inflection point: the mass surveillance system of cyber-surveillance conducted by private companies and their use of Big Data that ends up in government hands.[45]

II. BACKGROUND

A. Professor Popper's Clouds and Clocks

The distinction between clouds and clocks is a significant one. Clocks have reliability and predictability, as represented by the pendulum clock (and digitized timekeeping, if Professor Popper were to reiterate his analysis today).[46] The clock has entered the vernacular as an orderly physical system through such descriptions as "clockwork precision."[47] Further, it is objective, with no need or use for subjective interpretation.[48]

Clouds, on the other hand, represent physical systems that are "highly irregular" and unpredictable, as evidenced by weather forecast predictions.[49] While science understands what clouds are, the discipline does not have sufficient understanding to accurately predict their movements.[50] Illustrations of a cloud include a "cluster of small flies or gnats" and human interaction in the form of a picnicking family with children and a dog, who are not organized and predictive during the course of the picnic.[51]

Clouds and clocks are set forth as the two extremes on a continuum of reliability.[52] There are numerous stages in between the two.[53] Professor

---

42. *See* United States v. Jones, 132 S. Ct. 945, 954–56 (2012) (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).
43. POPPER, *supra* note 26, at 208.
44. *See infra* Part III.D.
45. *See infra* Part III.F.
46. *See* POPPER, *supra* note 26, at 207.
47. *Id.* at 208.
48. *See id.* at 207–08.
49. *Id.*
50. *See id.*
51. *Id.* at 208–10.
52. *Id.* at 208.
53. *Id.*

Popper uses the changing seasons as an illustration of "somewhat unreliable clocks."[54] Animals are closer to clouds than plants, which are closer to clocks.[55] Popper even makes the distinction between puppy dogs and older dogs; puppies are closer to clouds than their older (and presumably wiser) brethren.[56]

The question Professor Popper asks is whether all systems are effectively subject to physical determinism, where all clouds are really clocks.[57] The physical determinist uses Newtonian physics and physical laws to argue against human freedom of choice.[58] The nightmare of physical determinism, according to Popper, is that we are all automatons, little cogwheels in a much larger clock enterprise.[59]

In determining whether humans have free will or are deterministic beings, Popper refers to quantum physics, which was used to argue that the world is a closed system, much like a type of clock characterized by precision and predictability.[60] Popper disagrees with philosophers who argues that physics shows the world is a closed system.[61] Instead, Popper says imprecision is still part of physics such that it is less a clock than a type of cloud.[62] Specifically, Popper suggests that scientists use trial and error, an imprecise system, to discover the truth, and that quantum physics has not obviated the need to do so.[63] In fact, Popper views the scientific method as a trial-and-error system that creates a cloud-like control over a cloud system.[64] His conclusion is that humans are more like clouds than clocks, and that control over human behavior requires temporary plastic controls, meaning human-made controls that are less precise and predictable than a clock.[65]

Professor Popper also concludes that physical indeterminism is an appropriate model for living organisms, augmented by new theories of evolution and new models.[66] Consequently, Professor Popper argues that the world is neither a closed physical system nor one strictly of chance, but rather something in between.[67] Instead, there is human freedom of choice based on deliberate decisions.[68]

---

54. *Id.*
55. *Id.*
56. *Id.*
57. *See id.* at 222–26.
58. *Id.*
59. *Id.* at 222.
60. *Id.* at 217–18.
61. *Id.* at 218–19.
62. *Id.* at 213–14.
63. *Id.* at 234. Popper also offers the application of his view to art to evidence its cloud-like propensities. *Id.* He opines that for someone like Beethoven or Mozart, their own system of musical evaluation controls them—a form of "taste" that is still within the cloud family, not clocks. *Id.* at 254.
64. *Id.* at 234.
65. *Id.* at 232.
66. *Id.* at 242.
67. *Id.* at 231–32.
68. *Id.* at 254–55.

Professor Popper's solution to the model of the organism is especially useful in the Fourth Amendment context.[69] In Professor Popper's general theory, he suggests that "[a]ll organisms are constantly, day and night, engaged in problem-solving."[70] He says that each "organism can be regarded as a hierarchical system of plastic controls—as a system of clouds controlled by clouds."[71] Popper asserts: "The controlled subsystems make trial-and-error movements which are partly suppressed and partly restrained by the controlling system."[72] While mistakes are inevitable and expected, physicist John Archibald Wheeler noted, "Our whole problem is to make the mistakes as fast as possible."[73]

Professor Popper shows that plastic controls exist through examples of a Peircean system or a "soft" plastic control he calls a "soap bubble,"[74] keeping with his view that the physical world is an open system consistent with "the emergence of biological novelty and the growth of human knowledge and human freedom."[75] This view sheds light on the organic growth of advancing technology—accompanied by the government's use of it—and how the Fourth Amendment needs to be interpreted as a soft plastic control—a cloud that controls another cloud.[76]

The rest of this Article uses Professor Popper's approach to structure an argument about how the Fourth Amendment ought to limit police tracking.[77] To rein in police activity such as tracking, in light of exponential advances in technology, cloud controls imposed by the Supreme Court will be necessary, even if they evolve as a form of trial and error.[78]

B. The Design of the Fourth Amendment as a Cloud Limitation on Police Tracking

The premise of this Article is straightforward. The Fourth Amendment was intended to be a limitation on an organic and developing government, requiring some checks and balances as a regulatory limitation on government while also respecting the division between the public and private spheres.[79] It also is an integrity provision—limiting the actions of government even for

---

69. *See supra* text accompanying notes 52–59.

70. POPPER, *supra* note 26, at 242.

71. *Id.* at 245.

72. *Id.* One example he gives about how this works is "between the lower and higher functions of language." *Id.*

73. *Id.* at 247.

74. *Id.* at 248–49.

75. *Id.* at 255.

76. *See supra* text accompanying notes 37–39.

77. *See* discussion *infra* Part III.

78. Riley v. California, 134 S. Ct. 2473, 2487 (2014) (recognizing the cell phone as needing a cloud-like control).

79. *See supra* notes 37–39 and accompanying text (discussing how the Fourth Amendment is seen as a regulatory protection against government intrusion and transgression into the private sphere).

legitimate goals if the means are not equally legitimate.[80] This conceptualization applies to the Fourth Amendment, which protects "the people" and their "right . . . to be secure" from unlawful searches and seizures.[81] The Fourth Amendment does not specify where and when, but canons of interpretation have created a tapestry by which to understand the Fourth Amendment's application.[82]

1. Canons of Interpretation

The text of the Constitution supports this thesis.[83] "The people" are not directly protected from unreasonable searches and seizures but are given "the right . . . to be secure in their persons, houses, papers, and effects" through limits on search and seizure.[84] Thus, the end is security through a variety of search and seizure means.[85] This collective security is not achieved by the government as a protector but rather by limits placed on government.[86] While the notion of security might be amorphous, it is an important component of the Fourth Amendment, guaranteeing a private sphere that forbids uninvited eyes and ears of government without legitimate justification.[87]

The historical record also reinforces the use of the Fourth Amendment as a limitation on intrusive government practices in the private sphere. Unlike the general warrants permitted in England in the 1700s, no such expansive intrusion was desired in America.[88] States also included their own versions of the Fourth Amendment in their constitutions.[89] Without the Bill

---

80. *See supra* notes 37–39 and accompanying text. In this respect the Fourth Amendment is connected to the rational basis scrutiny used in equal protection and due process contexts—if the means are illegitimate, they still do not justify legitimate ends, even if in a criminal investigation the illegitimate means yield considerable contraband. *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 647 (1999).

81. U.S. CONST. amend. IV.

82. *See, e.g.*, Katz v. United States, 389 U.S. 347, 370 (1967).

83. *See* discussion *infra* notes 84–86.

84. U.S. CONST. amend IV.

85. *See, e.g.*, *Katz*, 389 U.S. at 353.

86. *See id.* at 365–66 (Black, J., dissenting).

87. *See, e.g.*, *id.* at 358–59 (majority opinion).

88. Davies, *supra* note 80, at 624–25 (discussing the necessary justification for searches).

89. *See, e.g.*, CONST. OF FORM OF GOVERNMENT FOR THE COMMONWEALTH OF MASS. of 1780, art. XIV, *reprinted in* 3 THE FEDERAL AND STATE CONSTITUTIONS: COLONIAL CHARTERS AND OTHER ORGANIC LAWS OF THE STATES, TERRITORIES, AND COLONIES NOW OR HERETOFORE FORMING THE UNITED STATES OF AMERICA 1888, 1891 (Francis Newton Thorpe ed., 1909) ("Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.").

of Rights, of which the Fourth Amendment plays a prominent part, there likely would not have been a deal for ratifying the Constitution.[90]

The colonists opposed writs of assistance and general warrants because of their lack of particularized suspicion.[91] They were equally against search warrants that were issued without justification.[92] Colonial protests provide evidence of the importance of particularized government suspicion to engage in searches and seizures.[93] As Justice O'Connor observed, "[T]he individualized suspicion requirement has a legal pedigree as old as the Fourth Amendment itself."[94]

2. Supreme Court Interpretations

The Supreme Court's interpretation of the Fourth Amendment further illustrates the importance of and need for cloud controls for the Fourth Amendment to serve its literal purpose of security for the people in their persons, houses, papers, and effects.[95]

a. Katz v. United States

In *Katz v. United States*, Justice Stewart updated the interpretation of the Fourth Amendment to incorporate the then-modern world of phone booths.[96] In *Katz*, the Government used electronic surveillance to overhear a person talking in a public phone booth.[97] The Court found that the prior *Olmstead* and *Goldman* trespass doctrine underpinnings, which focused on whether the Government was engaging in a physical trespass, were so eroded that they were no longer controlling.[98] The Court held that an enclosed telephone booth is an area where, like a home, a person has a constitutionally protected reasonable expectation of privacy, and that electronic, as well as physical, intrusions into a place that is private may constitute a violation of the Fourth Amendment.[99]

Justice Harlan's concurrence presented the still viable, two-pronged *Katz* test: (1) actual subjective expectation of privacy and (2) an expectation that society is prepared to recognize as reasonable.[100] Justice Harlan stated

---

90. *See Constitution*, BILL RIGHTS INST., http://billofrightsinstitute.org/founding-documents/Constitution/ (last visited Sept. 23, 2015). James Madison promised a quid pro quo to states if they ratified the Constitution—a Bill of Rights as amendments. *Id.*

91. *See* Davies, *supra* note 80, at 601.

92. *See, e.g.*, *id.* at 624–25.

93. *See id.* at 680–81.

94. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 678 (1995) (O'Connor, J., dissenting).

95. *See* Riley v. California, 134 S. Ct. 2473, 2482 (2014).

96. Katz v. United States, 389 U.S. 347, 348 (1967).

97. *Id.*

98. *Id.* at 353.

99. *Id.* at 353, 359.

100. *Id.* at 361 (Harlan, J., concurring).

that objects, activities, or statements exposed to the "'plain view' of outsiders are not 'protected'" because there is no intention to keep them to oneself.[101] The case appeared to be progressive, applying rules to the new electronic age.

Yet as expansive as the case's protection seemed, it contained language that has turned out to be quite limiting for protection.[102] The Fourth Amendment does not protect what a person knowingly exposes to the public, even in a person's own home or office.[103] While the day of the phone booth has since passed, *Katz* still reigns with no replacement test in sight.[104]

The reasonableness test of *Katz* is also fluid, as was seen in the aftermath of the terrorist attacks of September 11, 2001.[105] Those events can be helpful or not. For example, retired General Michael Hayden, who was the director of the National Security Agency, said:

> I know this is fact. What I viewed as reasonableness on the morning of September 10th, I viewed in a very different light on the afternoon of September 11th at the National Security Agency and I actually started to do different things. And I didn't need to ask 'Mother may I' from Congress or the President or anyone else. It was within my charter.[106]

b. The Supreme Court's Third-Party Rule

More than fifty years ago, the Supreme Court laid the groundwork for a significant narrowing of constitutional privacy rights that has come to be called the "third-party rule."[107] In *United States v. Miller*, the Court found that the defendant had a distillery with the capacity to make 7,500 gallons of illegal alcohol.[108] The defendant had, in fact, made 175 gallons. To assist in proving Miller's complicity, the Government subpoenaed his bank records. The Bank Secrecy Act requires that banks maintain the records of every customer's check and deposit for six years or longer.[109] Consequently, by law, the bank had Miller's incriminating records.[110] The Court held that the

---

101. *Id.*

102. *See id.* at 351 (majority opinion).

103. *Id.*

104. *See id.* at 359. *But see* Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring) (noting that while *Katz* is still good law, Congress has enacted legislation that governs electronic surveillance).

105. WASH. & LEE SCH. OF LAW, *W&L Law Cybersurveillance Symposium Keynote: Gen. Michael Hayden*, YOUTUBE (Jan. 23, 2015), https://www.youtube.com/watch?v=VUEuWiXMkBA.

106. *Id.* (General Hayden's comments begin at 8:55).

107. United States v. Miller, 425 U.S. 435, 437 (1976), *superseded by statute*, Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified as amended at 12 U.S.C. § 3401 (2010)), *as recognized in* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984).

108. *Id.*

109. *See* Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1116 (codified as amended at 12 U.S.C. § 1951 (1998)).

110. *Miller*, 425 U.S. at 438.

defendant's bank records could be subpoenaed and that the Fourth Amendment did not apply to the disclosure.[111] The Court placed the risk on the customer who assumed the risk of disclosure.[112]

Smith v. Maryland provided the other major bookend for the third-party rule of "knowing disclosure."[113] *Smith* involved a government pen register placed on the defendant's phone, but its facts are significant.[114] The case revolved around a criminal investigation for robbery. The victim received harassing and threatening calls after being robbed from a man identifying himself as the robber. At the police's request, the telephone company installed a pen register on the petitioner's phone at their central offices. Records revealed that the petitioner called the victim's phone. The Court found that a pen register had limited capabilities and that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[115] Because the information was voluntarily turned over to third parties, the Court held that there was no legitimate expectation of privacy in the phone numbers called.[116]

c. The Beeper Cases

The beeper cases are instructive on how Fourth Amendment doctrine relates to police tracking.[117] In the first major tracking case using a beeper, *United States v. Knotts*, Justice Rehnquist considered the validity of electronic tracking.[118] In *Knotts*, a codefendant of the respondent was suspected of stealing chemicals from his former employer, the 3M Company,[119] to be used in creating drugs, specifically methamphetamine.[120] Visual police surveillance showed that the codefendant also purchased the same chemicals from the Hawkins Chemical Company, who agreed to place a police radio transmitter in a five-gallon drum when the codefendant next purchased chemicals from them.[121] Officers tried tracking the drum through visual surveillance but lost the suspect after evasive maneuvers. Relying on the tracking device, the police traced the drum, which the codefendant

111. *Id.* at 445–47.

112. *Id.* at 443. Yet, the Government required that the bank keep the records and then sought access to the information without constitutional scrutiny. *Id.* at 436–37.

113. Smith v. Maryland, 442 U.S. 735, 744 (1979).

114. *Id.* at 737.

115. *Id.* at 742.

116. *Id.* at 745.

117. *See* United States v. Jones, 132 S. Ct. 945, 952–53 (2012); United States v. Knotts, 460 U.S. 276, 278–79 (1983).

118. *Knotts*, 460 U.S. at 280–85.

119. *Id.* at 278.

120. *Id.* at 279.

121. *Id.* at 278.

transported to the respondent's remote cabin. While the police lost the tracking signal for a while, they used a helicopter to get the signal back.

In *United States v. Jones*, a case with the potential to impose plastic cloud controls on the limits of electronic tracking through a satellite-based monitoring (SBM) system, Justice Scalia instead relied on the trespass test erected in *Olmstead v. United States* and virtually abandoned decades ago in *Katz*.[122] *Olmstead* was one of the leading cases that concluded that a physical trespass is a violation of the Fourth Amendment.[123] Justice Scalia built his case by referring to the classic, centuries-old case that provides a foundation for the Fourth Amendment, *Entick v. Carrington*, an English case from 1765.[124]

Justice Alito, in his concurrence, asserted that the holding was highly artificial and unwise.[125] The real question for Justice Alito was whether the long-term monitoring of the respondent's vehicle movements violated the respondent's reasonable expectation of privacy.[126] Justice Sotomayor, in principle, agreed.[127] Her concurrence also recognized that a non-trespass use of a GPS monitoring system could be a search in violation of the Fourth Amendment and violate its strictures.[128] In this way, Justices Alito and Sotomayor clearly recognized that the tracking posed a cloud problem and needed some kind of cloud control.[129]

C. The Problem: New Clouds of Mass Surveillance

There are multiple reasons why police tracking in the digital age raises complex and thorny Fourth Amendment issues. Today, tracking involves efficient and numerous opportunities for government data collection, either directly by the government or through private companies, utilizing the tacit consent of individuals.[130] Those companies aggregate and crunch information through Big Data, sifting through vast buckets of seemingly unrelated bits of information to develop clues about people's habits and propensities.[131] These issues are not only about the ease by which information can now be collected, how it can be re-aggregated and analyzed, or how it can be kept as a dossier forever, but also the issues run large to

---

122. *Jones*, 132 S. Ct. at 952–53; *see* Katz v. United States, 389 U.S. 347, 353 (1967).

123. *See* Olmstead v. United States, 277 U.S. 438, 457 (1948), *overruled by* Berger v. New York, 388 U.S. 41 (1967), *and* Katz v. United States, 389 U.S. 347 (1967).

124. *Jones*, 132 S. Ct. at 949 (citing Entick v. Carrington (1765) 95 Eng. Rep. 807 (K.B.)).

125. *Id.* at 958 (Alito, J., concurring).

126. *Id.*

127. *Id.* at 955 (Sotomayor, J., concurring); *see id.* at 964 (Alito, J., concurring).

128. *Id.* at 955 (Sotomayor, J., concurring).

129. *See id.*; *id.* at 964 (Alito, J., concurring).

130. *See* Soghoian, *supra* note 15, at 390–91.

131. Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 65–66 (2013), http://www.stanfordlawreview.org/sites/default/files/online/topics/66_StanLRevOnline_65_KerrEarle.pdf.

foundational and systemic questions involving the separation of powers.[132] As Justice Sotomayor stated in her concurrence in *United States v. Jones*:

> The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[133]

Even one branch of the government can track other branches without limit.[134] Further, government secrets tend to multiply, not result in a natural shift toward transparency.[135]

Professional police departments engage directly in mass surveillance, from license tag readers[136] to the use of drones,[137] Stingrays,[138] or other cell tower imitators such as Triggerfish.[139] But police also obtain their tracking information from another potentially pernicious form of mass surveillance conducted by private companies.[140] These private companies track their users in cyberspace, retail stores, and even their psyches and health.[141] Health tracking has become very popular, from nutrition tracking to heartbeat rhythms and sleep patterns.[142] The new voice-activated Samsung television

---

132. *See* Alicia Shelton, *A Reasonable Expectation of Privacy Online: "Do Not Track" Legislation*, 45 U. BALT. L.F. 35, 42–43 (2014).

133. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated,* 132 S. Ct. 1534 (2012)).

134. *See, e.g.*, Brian Fung, *NSA Refuses to Deny Spying on Members of Congress*, WASH. POST (Jan. 4, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/04/the-nsa-refuses-to-deny-spying-on-members-of-congress/.

135. *See generally* Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall"*, 17 STAN. L. & POL'Y REV. 437 (2006) (suggesting that there is a growing trend for the federal government to keep its operations secret from the public).

136. *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, ACLU.COM, https://www.aclu.org/feature/you-are-being-tracked (last visited Sept. 29, 2015).

137. *Domestic Drones*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones (last visited Sept. 29, 2015).

138. *Stingray Tracking Devices*: *Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Sept. 29, 2015).

139. Kim Zetter, *Secrets of FBI Smartphone Surveillance Tools Revealed in Court Fight*, WIRED (Apr. 9, 2013, 6:30 AM), http://www.wired.com/2013/04/verizon-rigmaiden-aircard/.

140. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 67 (2013).

141. *Id.*

142. Milt Freudenheim, *More Using Electronics to Track Their Health*, N.Y. TIMES (Jan. 27, 2013), http://www.nytimes.com/2013/01/28/health/electronic-health-tracking-increasingly-common-researchers-say.html?_r=o.

comes with a warning—what is said in the room of the television might be recorded by the company and some third parties.[143]

Then there is the "Internet of Things,"[144] where companies have developed smart objects and homes that allow us to track ourselves in ways we never could before, from how many steps we take in a day—as exemplified by the Fitbit and many other self-tracking watches or appendages[145]—to how our hearts are beating.[146] Interconnected devices and the companies that make them store and access this information as well as learn from it to adapt to new circumstances.[147] The government has partnerships with these companies, like telephone companies, and has either been handed information, sometimes in exchange for other information, or worked surreptitiously with the companies to not have encryption for transmitted data or to leave in weak back doors to software.[148]

Tracking by private companies is ubiquitous and ambitious. It is also more dangerous because these companies can share and sell buckets of sensitive information to each other or the government.[149] Google, Apple, Adobe, Pinterest, Snapchat, Wickr, Wikimedia, LinkedIn, Microsoft, Twitter, Yahoo, Tumblr, SpiderOak, AT&T, Verizon, Comcast, and of course Facebook haul in buckets of data daily, and many of these companies share this information for a price.[150] Furthermore, apps used by millions of people, especially free ones, are not really free. The companies that provide them are also purveyors of information, acquiring access to the users' information and collecting, and sometimes transferring, that information as the currency of "information transfer" gains in value.[151]

American consumers are not especially happy about companies mining their data, according to a study by the Annenberg School for Communication of the University of Pennsylvania.[152] The study found that "[m]any Americans do not think the trade-off of their data for personalized services,

---

143. David Goldman, *Your Samsung TV is Eavesdropping on Your Private Conversations*, CNN MONEY (Feb. 10, 2015, 6:38 AM), http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/.

144. Dennis Kennedy, *Webbed World: Preparing for the 'Internet of Things'*, A.B.A. J., July 2014, at 29.

145. Amir Khan, *Making the Most of Your Fitbit*, U.S. NEWS & WORLD REP. (May 8, 2014), http://health.usnews.com/health-news/health-wellness/articles/2014/05/08/making-the-most-of-your-fitbit.

146. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 88 (2014).

147. *See* Shelton, *supra* note 132, at 40.

148. *See* Soghoian, *supra* note 15, at 385–88.

149. *See* Deborah Pierce & Linda Ackerman, *Data Aggregators: A Study of Data Quality and Responsiveness*, CAL. ST. U. NORTHRIDGE 3 (May 19, 2005), http://www.csun.edu/~dwm3265/IS312/DataAggregatorsStudy.pdf.

150. *See* Peter Segrist, *How the Rise of Big Data and Predictive Analytics Are Changing the Attorney's Duty of Competence*, 16 N.C. J.L. & TECH. 527, 549–54 (2015).

151. *See id.*

152. *See* Singer, *supra* note 37.

giveaways or discounts is a fair deal either."[153] Americans want control over what marketers can access online.[154]

III. PROPOSAL

A. Recognize that Police Tracking Even in Public Places Raises Fourth Amendment Cloud Issues Requiring Flexible Plastic Controls

Police tracking today is only a distant cousin of its pre-digital past. As noted, the physical pre-digital tracking took time and resources, and was not always consistent or accurate.[155] Further, it was not often objectively verifiable, with sustaining proof of actions often difficult to obtain or fleeting.[156] Today, police tracking is much easier and occurs through multiple sustaining systems.[157] Significantly, it can readily pierce the wall of a person's private identity, with an increasing array of tools by which to do so.[158] Without new controls over police tracking, it will become unchecked, perpetual, and more expansive.

In fact, simply claiming that the tracking was in public, from online purchases, doctor visits, pharmacy purchases, bank records, or employee records, ignores the reality that the aggregation and compilation of the information transgresses public and private boundaries and should be considered a search under the Fourth Amendment if the government accesses that information.[159] As Justice Sotomayor observed in her concurrence in *Jones*, "In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[160]

To deal adequately with changing realities of advancing technology, from cell phones, to drones, facial recognition software, and more, courts need not create an entirely new set of rules. Courts can use some of the seminal cases to deal with these new clouds and create controls over the different issues raised.[161] Existing rules, though, need to be adapted to

153. *Id.*
154. *Id.*
155. *See* Soghoian, *supra* note 15, at 384.
156. *See id.* at 385.
157. *Id.* at 386–87.
158. *Id.*
159. *See* Daniel Zwerdling, *Your Digital Trail: Does the Fourth Amendment Protect Us?*, NPR (Oct. 2, 2013, 1:00 PM), http://www.npr.org/sections/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment-protect-us.
160. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).
161. *See, e.g.*, *id.*

changing privacy expectations.[162] Justice Alito stated in his concurrence in *Jones*:

> In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[163]

Some of the seminal case law supports the view that the Fourth Amendment presents a cloud issue, requiring rules based on current facts, not facts from a society of the *Katz* era almost fifty years past.[164]

B. Adapt to Advancing Technology—Follow the Lead of Carney *and* Riley

California v. Carney illustrates how the Supreme Court uses preexisting principles to adapt to changing culture and technology.[165] The case involved a recreational vehicle (RV), a mobile home, used as both transportation and an abode.[166] The Court considered the question of whether it considered the RV to be an automobile or home for purposes of Fourth Amendment analysis.[167] The Court held that a mobile home is primarily a vehicle and that courts should consider it as such, subject to one major exception when people station it and use it entirely as a home.[168] Thus, the Court focused on the characteristic of mobility and its functionality, not the lexicon of "home."[169]

The recent Supreme Court decision in *Riley v. California* illustrates how the Court can create a cloud control for an existing and well-established doctrine, such as search incident to a lawful arrest.[170] In *Riley*, the Court had to determine whether cell phones were subject to a search incident to a lawful arrest.[171] Were cell phones like the container found in *United States v.*

---

162. *See id.* at 962 (Alito, J., concurring).
163. *Id.*
164. *See id.* at 962–63.
165. *See* California v. Carney, 471 U.S. 386 (1985).
166. *Id.* at 393.
167. *Id.* at 387.
168. *See id.* at 394.
169. *See id.*
170. *See generally* Riley v. California, 134 S. Ct. 2473 (2014) (discussing the difference between a physical search of the subject and a search of the subject's cell phone data when there is no threat to safety or danger of destruction).
171. *Id.* at 2484.

Robinson, and subject to search, or were they qualitatively different and subject to a distinct rule?[172]

While the Court could have easily adopted the *Robinson* bright-line test, allowing a search as it did there with a crumpled cigarette package, it did not.[173] Instead, the Court interpreted the *Chimel v. California* line of cases, including *Robinson*, and adapted its outcome to modern facts.[174] These outcomes recognized the cloud nature of the Fourth Amendment and the import of not letting bright lines obfuscate the necessity for cloud controls.[175] Other suggested cloud controls follow. These controls are offered to provide legitimate limits on excessive and search-like police tracking.

C. Modify the Third-Party Rule to Reflect Limited Purpose Disclosures

Cloud controls can be created around several new inflection points. One such point involves recognizing a principle of limited disclosures.[176] This concept is reflected in the established practice of protecting evidentiary privileges.[177] Evidentiary privileges protect relationships where there is a reasonable expectation of privacy, such as attorney–client, psychotherapist–patient, and even accountant–client, and support limited purpose disclosures under the Fourth Amendment.[178] The notion of limited disclosures resonates in the digital world with online transactions becoming a focal point for social, financial, and political interaction—from complying with Facebook privacy requirements (or else be relegated to MySpace) to online pharmacy transactions to using financial institutions to assist with financial issues.[179] Furthermore, many transactions, even with third parties, are password protected.[180]

---

172. *Id.* at 2483–84, 2495. *See generally* United States v. Robinson, 414 U.S. 218 (1973) (holding that a search of a cigarette pack incident to a lawful arrest was reasonable under the Fourth Amendment).

173. *See Riley*, 134 S. Ct. at 2488–89.

174. *See id.* at 2484–95. *See generally* Chimel v. California, 395 U.S. 752 (1969) (holding that a reasonable search incident to a lawful arrest includes the subject's person and immediate area).

175. *Cf.* United States v. Jones, 132 S. Ct. 945, 953–54 (2012) (holding that use of GPS to monitor movements of a vehicle is a search); *Robinson*, 414 U.S. at 236 (holding that the search of a person incident to a lawful arrest is lawful); *Chimel*, 395 U.S. at 768 (holding that a search incident to arrest may only extend to the person and immediate, surrounding area).

176. *See* Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1089, 1091–92 (2006); *infra* notes 188–89 and accompanying text.

177. *See generally* Jaffee v. Redmond, 518 U.S. 1 (1996) (discussing the history and various types of evidentiary privileges).

178. *See id.* at 9–10.

179. *See* Soumava Bandyopadhyay, *Consumers' Online Privacy Concerns: Causes and Effects*, 8 INNOVATIVE MARKETING, no. 3, 2012, at 32, 33–34, http://www.businessperspectives.org/journals_free/im/2012/im_en_2012_03_Bandyopadhyay.pdf.

180. *See* John Adams, *What Will Replace the Password?*, AM. BANKER (Jan. 1, 2013), http://www.americanbanker.com/btn/26_1/what-new-technology-and-strategy-will-replace-the-password-1055356-1.html.

The evidentiary privilege analogue also argues for a continuum of privacy, not an all-or-nothing category, particularly for information such as that used for business or health matters.[181] Justice Marshall alluded to this notion of limited purpose disclosure and the flexibility of the private domain in his dissent in *Smith v. Maryland*, which Justice Sotomayor quoted in *Jones*: "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[182]

In *United States v. Miller*, Justice Brennan, in his dissenting opinion, noted that the transfer of financial information to a bank does not, in today's society, seem like a voluntary posting—certainly not, we can surmise today, similar to a posting on Facebook or a tweet to the world. Instead, it is a requirement of living on the grid and doing business in society.[183] It was necessary to use the bank to effectively participate in commercial society.[184] In essence, Justice Brennan argued that no voluntary unlimited transfer of information occurred.[185] At most, it can and should be seen as a bailment situation, where the bank was "possessing" the information on behalf of the owner.[186] Today, most transactions occur over the Internet, with electronic transfers or record-keeping.[187] Further, revealing financial information to a financial advisor is a far cry from the government obtaining that information for non-financial or government tracking purposes. The transfer of the information alone from a single private company to the government raises problems of potential misuse.[188] Justice Sotomayor noted that "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[189]

---

181. *See* Smith v. Maryland, 442 U.S. 735, 749 (1979).

182. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (quoting *Smith*, 442 U.S. at 749.)

183. *See* United States v. Miller, 425 U.S. 435, 450–52 (1976) (Brennan, J., dissenting) (quoting Burrows v. Superior Court, 529 P.2d 590, 593–96 (Cal. 1973)), *superseded by statute*, Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified as amended at 12 U.S.C. § 3401 (2010)), *as recognized in* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984).

184. *See id.*

185. *See id.*

186. *See id*. *But see In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012) (holding that a customer's personal information is not personal property and that possession of that information by a business does not constitute a bailment).

187. *See generally* Patricia Brumfield Fry, *Introduction to the Uniform Electronic Transactions Act: Principles, Policies and Provisions*, 37 IDAHO L. REV. 237, 238–39 (2001) (noting that electronic "transitions have become familiar to an ever escalating number of individuals").

188. *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

189. *See id.*

D. Limit Sustained Government Tracking Time Without Purported Justification to a Single Event or a Number of Hours

GPS mechanisms, drones, and cell phone location tracking permit sustained and ready tracking without justification.[190] Such tracking has eluded its natural predator—transaction costs. At the time of the adoption of the Fourth Amendment, there were pragmatic and sustainable limits on police tracking—time and resources.[191] Today, there are no similar costs.[192] Thus, there is an incentive for police departments to track, gather, and analyze without limit, so long as the costs are minimal.[193]

While individual bits of information might be exposed to the public, when sewn together, the tapestry at some point can readily create an intimate picture that could only be replicated in the most private recesses of a person's proprietary locus—the home.[194] By tracking a person's whereabouts over a period of time, what is revealed includes real-time consumer preferences, finances, political or partisan values, and photos of health—what doctors are being visited and personal preferences, from stores and other places frequented.[195] The problem is that this picture only becomes more intimate and detailed over time, without any oversight, restrictions, or even cataloguing.[196] This violates the spirit, if not the letter, of the Fourth Amendment.

Instead, *Knotts* provides a cloud limit of direct public tracking by drone, GPS, Internet, or other electronic substitute for physical surveillance.[197] The *Knotts* case gives us the one-trip rule.[198] Thus, a license plate reader at a fixed location would be okay, but not a GPS tracker honing in on a particular individual without cause.[199] Consistent with *Knotts*, Justice Alito in *Jones* stated: "Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."[200] But the use of longer term GPS

---

190. *See generally Cellphone Tracking Cases Highlight Privacy Concerns in Digital Age*, RT (Aug. 20, 2013, 5:51 PM), http://rt.com/usa/cellphone-tracking-privacy-concerns-701/ (noting the broad powers of the government to conduct tracking).

191. *See* Soghoian, *supra* note 15, at 384.

192. *See id.* at 387–88.

193. *See id.*

194. *See, e.g.*, Brad Turner, *When Big Data Meets Big Brother: Why Courts Should Apply* United States v. Jones *to Protect People's Data*, 16 N.C. J.L. & TECH. 377, 383–95 (2015) (detailing a multitude of ways in which tracking is employed).

195. *See id.*

196. *See id.* at 395–98.

197. *See* United States v. Knotts, 460 U.S. 276, 283–84 (1983).

198. *See id.* at 385; People v. Weaver, 909 N.E.2d 1195, 1199–1200 (N.Y. 2009) (noting that *Knotts* was limited to a tracking device used for a single trip).

199. *See Knotts*, 460 U.S. at 385.

200. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

monitoring in investigations of most offenses impinges on expectations of privacy.[201]

If the one-trip rule proves to be too varied, traffic stops provide a useful analogue. The general amount of time within which a traffic stop must be conducted is fifteen to twenty minutes.[202] If individuals are held longer than that time, the stop is considered a seizure for which there must be an adequate justification.[203] Similarly, for tracking that extends beyond one or two hours, a similar limit should exist. Individuals do not expect to or actually feel free under the First or Fourth Amendment when knowingly watched for any sustained length of time. Instead, feeling self-conscious and nervous after seeing a government tracker would be expected in the dominant culture.

1. Limit Aggregation of Data as Well

Tracking is not only linear today, with a police officer in pursuit of a suspect, but it involves horizontal scaling through Big Data as well.[204] To deal with current realities, the aggregation of data ought to be considered a search at a certain point as well. If this principle is adopted, time, place, and circumstance controls can provide a Popper-like cloud control for when the line of a search is crossed.[205] This theory can establish controls much like the time, place, and manner construct of indirect speech control in the First Amendment.[206] The Court is good at establishing presumptions of constitutionality through different levels of scrutiny.[207]

2. Maintain Checks and Balances

Another inflection point is the concern about visibility and remedy—the courts (and legislatures) cannot regulate what they cannot see. Justice Sotomayor said in her concurrence in *Jones*:

> I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance."[208]

---

201. *See Knotts*, 406 U.S. at 283–84.
202. *See* United States v. Sharpe, 470 U.S. 675, 683 (1985).
203. *See* Rodriguez v. United States, 135 S. Ct. 1609, 1614–15 (2015).
204. *See* Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 832–33 (2015).
205. *See* Grayned v. City of Rockford, 408 U.S. 104, 115 (1972).
206. *See id.*
207. *See* Nordlinger v. Hahn, 505 U.S. 1, 17 (1992).
208. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

This consideration raises a separation of powers issue and requires some check, notably the Fourth Amendment, if entire programs are not subject to judicial review or congressional control.

E. Limit Who Can Have Access to Tracking Information and How Long It Can Be Retained

Limits must be placed not only on the initial tracking but also on what is done with government-acquired information. Simply because the government has obtained access to information does not mean that information is now permanently part of the government's cache.[209] The government should delete or cabin some information. Evidentiary standards are helpful markers for who can obtain access to tracking information. The law provides evidentiary privileges to protect relationships, such as attorney–client, clergy–penitent, and psychotherapist–patient, even though some information is divulged to third parties through assistants, billing, and other indirect ways.[210]

If there is a psychotherapist–patient privilege, then similar limits should be applied to tracking without any legitimate justification. This means that a person whom the government tracks going into a psychotherapist's office should be secure from government follow-up or exploration if there is no legitimate basis, a reasonable suspicion, or probable cause, to do so.

F. Apply Effective Remedies to the Gathering, Storing, and Analyzing of Private Information

If it is to ensure that "the people" are secure in their persons, houses, papers, and effects, the modern Fourth Amendment must apply to more than just evidence offered in a criminal case. Because so much information collected today is not backward-looking, vertical information but forward-looking, preventive, horizontal information, like a linked data cloud, the Fourth Amendment should extend to evidence accessed, gathered, stored, or crunched by the government.[211] A violation in the modern world should not just be used in a criminal case, as defined in the exclusionary rule, but it should also be the use of information to derive clues of propensities to commit possible future crime.[212] Big Data is a new tool for prediction, but

---

209. *See* United States v. Ganias, 755 F.3d 125, 137–38 (2d Cir. 2014), *reh'g granted en banc*, 791 F.3d 290 (2d Cir. 2015).

210. *See* Jaffee v. Redmond, 518 U.S. 1, 2 (1996); Upjohn Co. v. United States, 449 U.S. 383, 389–97 (1981).

211. *See generally* DATAVERSITY, http://www.dataversity.net (last visited Sept. 29, 2105) (discussing the use and management of data).

212. *See* THE BOURNE SUPREMACY (Universal Pictures 2004). The experience of intrusion matters, not just the use of evidence in a criminal case. *See id.* In *The Bourne Supremacy*, for example, one scene is illustrative. Jason Bourne is talking on the phone with Pamela Landy, the CIA operative, in NYC. *Id.*

it is just that, a human-run tool that must fit within constitutional limitations when the government controls or uses it, not something that rises above the Constitution, creating reliability from its algorithms.[213] As Justice Sotomayor observed in her concurrence in *Jones*, it is what the government does with the information collected that matters:

> The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[214]

IV. CONCLUSION

Police tracking in the pre-digital age had numerous natural limitations.[215] Without these limits today, the police and the government will try to access as much data as possible from private citizens.[216] The citizens might be suspects, might become suspects, or might not serve any threat at all.[217]

Today, we are conditioned to disclose information as long as we consent to live on the societal grid—to be social or to obtain medical, pharmaceutical, financial, tax, and other essential services. We also live in a culture of tracking, regardless of suspect status.[218] Everyone is engaged in tracking in some way, including government, private companies, friends, family, and even us. In light of this new age of technology, Professor Karl Popper's approach to the human condition as a division between clouds and clocks provides a useful analogue.[219] The changing technology has created new clouds over the Fourth Amendment, consequently requiring new cloud controls.[220] As society changes, the Fourth Amendment must be adapted to new realities.

As the conversation ends, Bourne tells Landy she looks tired and should get some sleep. *Id.* Her look of panic as a result of being spied on says it all—she feels violated. *Id.*

213. *See generally* Turner, *supra* note 194 (discussing the constitutionality of the government's use of Big Data).

214. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 132 S. Ct. 1534 (2012)).

215. *See supra* notes 1–6 and accompanying text.

216. *See supra* notes 7–25 and accompanying text.

217. *See supra* notes 1–19 and accompanying text.

218. *See supra* notes 7–19 and accompanying text.

219. *See supra* Part II.A.

220. *See supra* Part III.