SPEECHES

SYMPOSIUM KEYNOTE ADDRESS

*Jeffrey Rosen**

It is hard to think of a more timely topic than the Fourth Amendment and emerging technologies. And just this week, at a time when everyone was focused on the gay marriage decisions, the Supreme Court gave us an important decision in a case involving a dog sniff on a front porch that provides both a window into constitutional limitations on ubiquitous surveillance and also highlights the shortcomings of then current doctrine.[1] In our conversation this morning, I'd like to imagine the kind of ubiquitous surveillance that we are already experiencing as citizens across the globe and think through with you the following question: Would ubiquitous 24/7 surveillance be unconstitutional under current Supreme Court doctrine and, if not, as I reluctantly conclude it is not, what would an alternative to the Supreme Court's approach be?

I would like to begin with a hypothetical, which is increasingly not so hypothetical. I was at a conference at Google in 2007 and the head of public policy, who later became a White House technology advisor, said he imagined that within just a few years, Google and Facebook would be asked to provide live and online streams to public and private surveillance cameras in the world. There are already, as you know, individual live streams you can sign into online. Facebook has a webpage that lets you sign on to beach cameras in Mexico,[2] for example. But the Google official asked us to imagine what would happen if the Mexican beach cameras were linked to the Washington, DC, subway cameras, which were linked to the London hospital cameras, and all of these live feeds were archived and stored. It would then be possible to click on a picture of someone anywhere in the world—say, me—"back click" on me to see where I had been coming from, "forward click" to see where I was going, and basically have ubiquitous 24/7 surveillance of anyone in the world at all times. So that seemed a little like science fiction in 2007. But today, it's not

* Professor of Law, The George Washington University Law School.

1. *See* Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013).

2. *See Akumal Beach Web Cam: LocoGringo Riviera Maya Hotels, Resorts, and Vacation Rentals in the Mexican Caribbean,* FACEBOOK, https://www.facebook.com/RivieraMayaBeachCam (last visited Oct. 24, 2013).

science fiction. Google, as you know, has announced the development of "Project Glass," the next generation of a device that will allow people to record live encounters and store these encounters forever in the digital cloud.[3] It is not impossible that, in a few years, a social norm will develop that requires people to ask each other whether or not they are allowed to be recorded in every public and private encounter. And of course, these images will be increasingly archived and stored.

Or take the other constitutional controversy of the month, drone technology, which can be used not only for targeted assassinations,[4] but also for ubiquitous tracking.[5] And as police departments increasingly begin to use drone technologies to track individual suspects 24/7,[6] or to put areas of the country under permanent surveillance, this possibility of 24/7 tracking will become increasingly real. This is not science fiction and this is why it is so important that your symposium has gathered to address the question: Would ubiquitous surveillance, if installed tomorrow by Google or by Facebook, violate the Fourth Amendment to the Constitution?

The Fourth Amendment, as you know, says "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[7] Let's imagine, first of all, that the government is using this 24/7 Google surveillance system to track suspected terrorists. I'm using that as an example because Google and Facebook are private companies; they are not themselves bound by the Fourth Amendment.[8] If Mark Zuckerberg decided it was just a cool new app to let people check up on their friends, you might argue that this 24/7 surveillance system, call it Open Planet, wouldn't implicate the Fourth Amendment at all because there is no state action.[9] But for our purposes, let's imagine that the government is using Open Planet to track suspected terrorists and we have overcome the state action problem and the Fourth Amendment is implicated. Is there an unconstitutional search if the government tracks me 24/7 for a month using the Open Planet system? As I mentioned, the *Jardines*

3. Associated Press, *Google to Meld Human and Goggle with New Project*, ABC LOCAL (Apr. 6, 2012), http://abclocal.go.com/ktrk/story?section=news/technology&id=8609753.

4. *Targeted Killings*, ACLU, https://www.aclu.org/national-security/targeted-killings (last visited Oct. 31, 2013).

5. *See* Somini Sengupta, *Lawmakers Set Limits on Police in Using Drones*, N.Y. TIMES, Feb. 16, 2013, at A1.

6. *See id.*

7. U.S. CONST. amend IV.

8. *See, e.g.*, Kevin L. Cole, *Federal and State "State Action": The Undercritical Embrace of a Hypercriticized Doctrine*, 24 GA. L. REV. 327, 327 (1990).

9. *Id.*

decision, which the Supreme Court just handed down, casts some light on this question. This was a case where the cops suspected that a guy might be growing pot, but didn't have probable cause for a warrant, so they took a drug-sniffing dog on his front porch.[10] This is a big dog, with a six-foot leash. The dog goes crazy and alerts, and based on the alert, the police get a warrant and find that he is indeed growing marijuana.[11] He objects, arguing that the dog sniff on his porch was an unconstitutional search.[12] In an ideologically eclectic majority opinion, Justice Scalia, writing for the Court, agreed that there was a search.[13] He said that "[w]hen 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a "search" within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'"[14] "That principle renders this case a straightforward one," Justice Scalia continued.[15]

> The officers were gathering information in an area belonging to Jardines and immediately surrounding his house—in the curtilage of the house, which we have held enjoys protection as part of the home itself. And they gathered that information by physically entering and occupying the area to engage in conduct not explicitly or implicitly permitted by the homeowner.[16]

So the focus was on physical intrusion. "The officers learned what they [did] only by physically intruding on Jardines' property to gather evidence" and that was "enough to establish that a search occurred."[17]

Of course, the focus on physical intrusion tells us little about the Open Planet situation because the government in that case doesn't have to physically intrude on me in order to track me 24/7—it just aggregates and collects the Google Glass feeds or the drone cameras—and, according to this *Jardines* test, there would be no Fourth Amendment issue at all.

Justice Elena Kagan wrote an extremely provocative and also very colloquial and well-written concurrence.[18] She would have focused not only on the property interest but also on the privacy interest, invoking the *Katz* "expectation of privacy" test.[19] She said:

> For me, a simple analogy clinches this case—and does so on privacy

10. Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013).
11. *Id.*
12. *See id.* at 1414.
13. *Id.* at 1412-18.
14. *Id.* at 1414 (quoting United States v. Jones, 132 S. Ct. 945, 950 n.3 (2012)).
15. *Id.*
16. *Id.*
17. *Id.* at 1417.
18. *See id.* at 1418-20.
19. *Id.* at 1418 (Kagan, J., concurring).

> as well as property grounds. A stranger comes to the front door of your home carrying super-high-powered binoculars. He doesn't knock or say hello. Instead, he stands on the porch and uses the binoculars to peer through your windows, into your home's furthest corners. It doesn't take long (the binoculars are really very fine): In just a couple of minutes, his uncommon behavior allows him to learn details of your life you disclose to no one. Has your 'visitor' trespassed on your property . . . ? Yes, he has. And has he also invaded your 'reasonable expectation of privacy,' by nosing into intimacies you sensibly thought protected from disclosure? Yes, of course, he has done that too.[20]

I love the immediacy of Kagan's writing. She is speaking directly to us in a way that the greatest justices have and she makes clear what she thinks is really at stake here, which is not just property, but also privacy. She said, "If we had decided this case on privacy grounds, we would have realized that *Kyllo* [] already resolved it."[21] In *Kyllo*, you will recall, the cops used a thermal-imaging device to detect heat emanating from a private home, even though they committed no trespass.[22] And she cites the *Kyllo* rule: "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[23] According to Justice Kagan, "[t]he police officers [in *Jardines*] conducted a search because they used a 'device . . . not in general public use' (a trained drug-detection dog) to 'explore details of the home' (the presence of certain substances) that they would not otherwise have discovered without entering the premises."[24]

This is a great concurrence and Kagan is reminding us not to rest purely on property but also on privacy and the *Katz* expectation of privacy test.[25] But again, we see the inadequacies of that test when it comes to Open Planet and to surveillance outside the home. First of all, if I were being tracked by drones or Google Glass feed outside the home, the *Kyllo* test would not apply. Furthermore, we can see the circularity of the test, which depends on technologies not in general public use. If Mark Zuckerberg announced tomorrow that he was starting Open Planet, or if the government just began to aggregate the Google Glass feeds, it would be easy to imagine in just a few years that this ubiquitous surveillance *would be* in general

---

20. *Id.* (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

21. *Id.* at 1419 (internal citations omitted).

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

23. *Jardines*, 133 S. Ct. at 1419 (quoting *Kyllo*, 533 U.S. at 40).

24. *Id.*

25. *Id.* at 1418; *see also Katz*, 389 U.S. 347 (1967).

public use and our expectations of privacy would be diminished along with our constitutional protections.

There is, furthermore, a very fiery dissent by Justice Alito,[26] who said (*a*) there is no trespassing problem because dogs have been around since fourteenth century Scotland and police are allowed to walk up to your home without committing a trespass,[27] and (*b*) there's also no *Kyllo* problem because members of the public don't expect that odors emanating from the house won't be smelled and detected by dogs or policemen.[28] This shows the inadequacy of property and expectation of privacy as a way of protecting us from ubiquitous surveillance.

That inadequacy was put into even sharper relief by the *U.S. v. Jones*[29] case, which seems to be concerned about the problem of ubiquitous surveillance but showed the inability of the Court to regulate it. *Jones*, of course, involved the cops' decision to place a GPS device on the bottom of a suspect's car without a valid warrant and to track his movements 24/7 for a month.[30] Based on ubiquitous tracking, they concluded he was a drug dealer.[31] They indicted and convicted him.[32] He objected on the ground that, because there was no valid search warrant, the search was unconstitutional.[33] In fact, the cops had gotten a search warrant, but they were supposed to serve it within ten days.[34] In fact, they started tracking him on the eleventh day.[35] Also, they were only supposed to follow him in DC, but in fact they followed him to Maryland.[36] So for the purposes of the case, the Court had to assume there was no valid warrant, and the Obama administration made it easier by taking the robust position that no warrant is ever required for 24/7 month-long GPS tracking because we have no expectation of privacy in public.[37] The Court unanimously rejected that sweeping holding, but again in a way that provides little guidance for how to regulate ubiquitous surveillance that doesn't involve a physical intrusion.[38]

Five members of the Court, again with Justice Scalia writing, held that because the government had physically intruded on Jones'

26. *Jardines*, 133 S. Ct. at 1420-26 (Alito, J., dissenting).
27. *Id.* at 1420, 1423.
28. *Id.* at 1425.
29. United States v. Jones, 132 S. Ct. 945 (2012).
30. *See id.* at 948.
31. *Id.*
32. *Id.* at 948-49.
33. *See id.* at 949.
34. *Id.* at 948.
35. *Id.*
36. *Id.*
37. *See id.* at 950.
38. *See id.* at 949.

effects, mainly his car, by affixing the GPS to the bottom of the car, a search had occurred.[39] That holding was insufficient for Justice Alito. Here, on the pro-privacy side, Alito noted that the government could have obtained the same geolocational information by subpoenaing the cell phone records from Mr. Jones' cell phone, or by subpoenaing the records from the low-jack device that might have been installed in his car.[40] He said focusing on physical intrusion was inadequate and he proposed a broader rule.[41] He said we do have an expectation of privacy in the whole of our movements over a month because month-long surveillance can reveal so much about us[42]—our political affiliations, our religious beliefs, the bars we visit, the friends we associate with. Therefore, he said, a warrant is presumptively required for month-long surveillance.[43] The cops can surveil people for a day without a warrant and if they're unsure about the precise moment a warrant is required, they should get one.[44]

On one level, Alito's concurrence seemed like a great victory for privacy because it escaped from the limitations of the focus on physical trespass. But on another, it failed to escape from the circularity of the expectation of privacy test. Alito once again relied on the presumption that citizens in fact don't expect to be tracked 24/7 because that sort of technology is not of general public use.[45] As soon as that technology becomes of general public use, then the expectation of privacy is defeated and then the constitutional protection evaporates.

There's a more serious problem with current doctrine that was identified by Justice Sonia Sotomayor in her extremely interesting concurrence in the *Jones* case. Sotomayor noted that cell phone locational data, which would have revealed as much about Mr. Jones' movements as the physical GPS device did, can presumptively be seized without a warrant because of so-called third-party doctrine.[46] Third-party doctrine, you remember from *United States v. Miller*,[47] says that when I disclose information to a third party for one purpose, I abandon all expectation of privacy in it for other purposes.[48] That was a case involving bank records where the Court said when I turn over financial information to the bank for my own depositing purposes I have to assume the risk that the bank will be

39. *See id.*
40. *See id.* at 962-64 (Alito, J., concurring).
41. *Id.* at 959-64.
42. *See id.* at 964.
43. *Id.*
44. *Id.*
45. *Id.*
46. *See id.* at 957 (Sotomayor, J., concurring).
47. 425 U.S. 435 (1976).
48. *Id.* at 442-44.

compelled to turn the matter over to the government.[49]

The *Smith*[50] case was likewise counterintuitive. Congress was so unhappy with it that it overturned it by statute,[51] but the broad principle of the *Smith* case continues to govern. And, at a time when most of us store our papers and effects not in locked desk drawers in the home but in third-party servers in the digital cloud, the third-party doctrine, as Justice Sotomayor suggested, means that we have no protection from the ability of the government to collect records of our geolocational movements.

Justice Sotomayor called for the third-party doctrine to be reconsidered but didn't provide a model for what exactly should replace it. What I would like to do now is think through what an alternative to the third-party doctrine and expectation of privacy test might be, which would protect us from the kind of ubiquitous 24/7 surveillance using Google Glass or drones that the Court thought was objectionable when it involved physical trespass.

So what are some alternatives to the third-party doctrine? Lower courts have begun to grapple with this question, asking whether cell phone geolocational data can be seized without a warrant.[52] In 2011, a federal district court in New York ruled that a warrant is required for law enforcement access to stored cell site information generated by the operation of a cell phone.[53] Judge Garaufis wrote the opinion in a case with a clumsy name: *In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*.[54] This is, however, a very interesting opinion. Judge Garaufis wrote, "The advent of technology collecting cell-site-location records has made continuous surveillance of a vast portion of the American populace possible: a level of Governmental intrusion previously inconceivable. It is natural for Fourth Amendment doctrine to evolve to meet these changes."[55] The decision was unusual because most current courts require probable cause for access to prospective location information that would allow real-time tracking.[56] This, by contrast, was an application for access to *stored* or "retrospective" or historical locational information about a

49. *Id.* at 443.

50. Smith v. Maryland, 442 U.S. 735 (1979) (holding that plaintiff did not have a reasonable expectation of privacy in dialed telephone numbers because such numbers are volunteered to the phone company).

51. 18 U.S.C. § 3121(a) (2012).

52. *See* Somini Sengupta, *Warrantless Cellphone Tracking Is Upheld*, N.Y. TIMES, July 31, 2013, at B1.

53. *In re* Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113 (E.D.N.Y. 2011).

54. *Id.* at 114.

55. *Id.* at 126.

56. *See, e.g.*, State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

person's movements in the past.[57] And it was interesting also because Judge Garaufis made a strong case for making an exception to the third-party doctrine for cumulative cell-site-location records. He found that there was a "content exception" to the third-party doctrine and that cumulative cell site location records are sufficiently sensitive that a similar exception should be created for those records.[58]

Although Judge Garaufis's opinion was creative, the analogy was necessarily imprecise. The content exception, which was recognized in cases in the wake of *Smith v. Maryland*, basically drew a distinction between content and envelope information.[59] Those cases said that while a third party may have physical control over an individual's information, this doesn't make all expectations of privacy unreasonable.[60] The only information a third party sees is the envelope information, the argument goes, but information remains protected when it is hidden from the third party—such as the content of letters.[61] Courts have tried to use this distinction between content and envelope information in the electronic age by trying to protect from warrantless disclosure things like the inside of a letter or the content of email, as opposed to dialing or pen register information.[62] So it was creative for Judge Garaufis to invoke the content exception to protect geolocational information, but the analogy is obviously strained because, after all, there is no distinction between content or envelope information when it comes to GPS locational information. This information is disclosed directly to the cell phone companies, which makes it seem like envelope information, but it reveals a great deal about us, which makes it seem more like content information. The lower court had to develop the analogy by saying that ubiquitous tracking is like content in the amount of information it can reveal, but the metaphor has limits because when we're tracking movements in public, it's the amount of information that is revealed, not the parties to whom it is revealed, that threatens privacy.[63] So although I

57. *In re Application of United States*, 809 F. Supp. 2d at 114.

58. *Id.* at 122.

59. *See generally* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105 (2009).

60. *See, e.g.*, *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("[A] distinction is to be made . . . between what is intended to be kept free from inspection, such as letters, and sealed packages . . . and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined. Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.").

61. *Id.*

62. *See* United States v. Forrester, 495 F.3d 1041, 1049-50 (9th Cir. 2007), *amended and superseded by* United States v. Forrester, 512 F.3d 500 (9th Cir. 2009).

63. *See In re Application of the United States*, 809 F. Supp. 2d at 126.

think this is a creative attempt to apply old metaphors in an electronic age, the metaphors themselves are inadequate.

What are other alternatives to the third-party doctrine? Another creative approach is proposed by Nita Farahany.[64] She uses intellectual property as a model and says that when individuals are the authors of information, the searches of their electronic effects should be both covered by intellectual property law and presumptively protected by the Fourth Amendment.[65] So her approach would protect emails, for example, not by distinguishing between content and non-content, but as electronic effects in which individuals have an intellectual property interest. But Farahany's approach, as she acknowledges, is inadequate to protect geolocational information.[66] This is the collection of automatically generated electronic evidence about individuals.[67] Individuals don't author these effects, they just emit them, and therefore the intellectual property model fails when it comes to the protection of our geolocational information and our cell phone records.[68]

Unsatisfied by the creative, but limited, existing proposals, I find myself asking the question I always do whenever I have a hard challenge in an effort to translate constitutional values in light of new technology and that is WWBD—What Would Brandeis Do? Justice Brandeis is my hero. He is, of course, the greatest prophet of the need to translate technologies in light of constitutional values. Brandeis set forth constitutional translation in his totemic dissent in the *Olmstead* wiretapping case from 1928.[69] *Olmstead,* like *Jones,* was an attempt by the majority of the Court to focus on physical trespass as a protection against electronic surveillance.[70] In *Olmstead*, at the height of Prohibition, the cops suspected a guy of being a bootlegger and they tapped the wires in the telephones under the public sidewalks leading up to his office.[71] The majority of the Court, in a formalistic opinion by Justice William Howard Taft, said no physical trespass, no Fourth Amendment problem.[72] Because the cops didn't physically have to intrude on Olmstead's office, but

64. *See generally* Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239 (2012).

65. *Id.* (arguing that an "intellectual property law metaphor better describes emerging [Fourth Amendment] doctrine").

66. *See id.* at 1286.

67. *Id.* at 1283.

68. *See id.* at 1286.

69. Olmstead v. United States, 277 U.S. 438, 471-85 (1928) (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

70. *Compare Olmstead*, 277 U.S. 438, *with* United States v. Jones, 132 S. Ct. 945 (2012).

71. *See Olmstead*, 277 U.S. at 455-57.

72. *See id.* at 466.

instead tapped the wires outside his office, there was no unreasonable search or seizure.[73] Brandeis disagreed. He said in stirring language that when the Fourth and Fifth Amendments were adopted, the evil that was to be avoided could only be achieved by physical intrusion into the home.[74] But, said Brandeis, "time works changes, brings into existence new conditions and purposes."[75] He continued, "[s]ubtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[76] And at this point Brandeis wanted to insert in his opinion a reference to television, which had just been invented, and he had a clipping that he had in his case file about the new invention of television.[77] But he slightly misunderstood the technology, or more accurately he was prescient and anticipated its evolution into a form of two-way video. He thought of it as a kind of Skype. Because this wasn't the way television worked at the time, his law clerk persuaded him to omit the reference. But Brandeis indirectly looked forward to both Skype and the age of cyberspace in his remarkable opinion. Brandeis said,

> "in the application of a Constitution, our contemplation cannot be only of what has been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[78]

Then he anticipated FMRI technology in brain scans: "Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions."[79] At the time of the framing he said, "far slighter intrusion seemed 'subversive of all the comforts of society.' Can it be that the Constitution affords no protection against such invasions of individual security?"[80]

This is a remarkable passage, both in its technological prescience and its insistence that the Fourth Amendment should protect the

---

73. *See id.*

74. *See id.* at 473-75 (Brandeis, J., dissenting).

75. *Id.* at 472-73.

76. *Id.* at 473.

77. Melvin I. Urofsky, *Mr. Justice Brandeis and the Art of Judicial Dissent*, 39 PEPP. L. REV. 919, 936 (2012) (citing NORMAN K. RISJORD, REPRESENTATIVE AMERICANS: POPULISTS AND PROGRESSIVES 192 (2005)).

78. *Olmstead*, 277 U.S. at 474.

79. *Id.*

80. *Id.* (footnote omitted).

same amount of privacy in the age of wiretapping, or Skype, or FMRI scans as it protected at the time of the Framers. He insisted that the Framers were concerned about protecting "unexpressed beliefs, thoughts and emotions,"[81] and they were concerned about political anonymity—in particular, the case of John Wilkes, a critic of King George who wrote in an anonymous pamphlet criticizing the king.[82] In those days, the only way of unmasking Wilkes' anonymity was to break into the homes of hundreds of suspects, to rummage through desk drawers and identify Wilkes as the author of the pamphlet.[83] In the Wilkes time, privacy was protected by the law of private property, and because there was no valid warrant, Wilkes was able to argue that he had been victimized by an unreasonable search and therefore he won a large trespass verdict.[84]

Although he tells the story of Wilkes, Brandeis resists the perils of formalism. He insists that we should focus on the values the Framers meant to protect—namely, a degree of personal anonymity in public, and the ability to control how much of our thoughts, emotions, and sensations are disclosed to others—rather than the particular technology deployed to invade these values. In his celebrated conclusion, Brandeis achieves a kind of constitutional poetry:

> The protection guaranteed by the [the Fourth and Fifth] amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. [85]

This paragraph, for me, provides the answer to the question I'm struggling with in looking for an alternative to the third-party doctrine. How is ubiquitous tracking an unjustifiable intrusion on the right to be let alone? In what sense do we have an expectation to privacy in public? I think Brandeis would have taken the paradigm

---

81. *Id.*

82. *See* David E. Steinberg, *An Original Misunderstanding: Akhil Amar and Fourth Amendment History*, 42 SAN DIEGO L. REV. 227, 259 (2005).

83. *See id.*

84. *See id.*

85. *Olmstead*, 277 U.S. at 478-79.

case, John Wilkes and the anonymous pamphlet, and said at the time of the framing, government could only obtain information about Wilkes's political beliefs, sensations, thoughts, and emotions by breaking into his house. Today, or tomorrow, the government will be able to obtain even more information about our political beliefs, sensations, thoughts, and emotions, and threaten our right to public anonymity even more acutely, by placing a drone camera on a political activist and tracking him 24/7. This 24/7 tracking, whether achieved through drones or Google Glass or Open Planet, violates a citizen's right to anonymity in public. The ability to maintain a degree of public anonymity against the government allows us to control how much information about our political and religious beliefs, thoughts, sensations, or emotions are disclosed to the public, and technologies that threaten this control are an unreasonable search of our persons and of our electronic effects.

I don't think the ruling has to be that much more elaborate than that. I think that Brandeis would sweep away the technicalities of the third-party doctrine and expectations of privacy and he would say that 24/7 surveillance of our movements for a month is an unreasonable search of our persons and our electronic effects. And of course, he would do it much more eloquently, but I don't think that doctrinally it really has to be much more complicated. I think he would cut the Gordian knot and remind us about the value that we are protecting which is a degree of anonymity in public.

Now Brandeis could, of course, have ruled even more expansively. He might have focused not only on the text of the Fourth Amendment, but he might have also seen 24/7 tracking as a violation of the liberty interest protected by the Due Process Clause.[86] After all, in Brandeis's first great article on the right to privacy he published in 1890, he said that the common law protects a "man's spiritual nature" and "his feelings and his intellect."[87] He said,

> Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.
>
> . . .
>
> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. . . . In every such case the individual is entitled to decide whether that which is his

86. *See* U.S. CONST. amend V.

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

shall be given to the public.[88]

The ability to control how much information about ourselves is communicated to others has been defined as the heart of the right to privacy by Alan Westin in his great book *Privacy and Freedom*.[89] Westin notes that this ability to control personal information includes separate interests in maintaining four states of privacy—solitude, intimacy, reserve, and anonymity.[90] I can imagine an expansive due process-like opinion saying that our interest in anonymity in public is threatened by ubiquitous surveillance and this defeats our ability to control how much of emotions, sensations, and thoughts are communicated to others. Brandeis, in his 1890 right to privacy article, talked about a more general right to the immunity of the person, the right to one's personality and he described a right to an inviolate personality.[91]

I can even imagine a sweeping opinion that would identify the right to an inviolate personality or more broadly some right to personal autonomy, and the cases it would cite would be cases like *Planned Parenthood v. Casey* and *Lawrence v. Texas*, the cases that upheld *Roe v. Wade* and recognized the rights of gays and lesbians to intimate sexual expression.[92] Justice Kennedy wrote those decisions and he famously said, "At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life."[93] Justice Scalia criticized Kennedy's language as the "sweet-mystery-of-life passage."[94] He thought it was too expansive, but it remains the law of the land and I don't think that it's a doctrinal stretch to say a natural home for a right of personal autonomy in public is the liberty protected by the Due Process Clause and recognized in autonomy cases like *Casey* and *Roe*.

But would Brandeis have taken that step? My sense here is that he might not. Brandeis did not like substantive due process because he didn't like *Lochner*.[95] He thought that by declaring a broad right to contract the Court had threatened democratic self-governance. He was generally very much in favor of deference to state legislatures as laboratories of democracy and was reluctant to strike down laws in the names of rights that weren't explicitly enumerated in the text of the Constitution. Brandeis made an exception, of course, for the textually enumerated First and Fourth Amendment rights, which he

88. *Id.* at 195-99.

89. Alan F. Westin, PRIVACY AND FREEDOM (1967).

90. *Id.* at 31-32.

91. Warren & Brandeis, *supra* note 87, at 211.

92. Planned Parenthood v. Casey, 505 U.S. 833 (1992); Lawrence v. Texas, 539 U.S. 558 (2003); Roe v. Wade, 410 U.S. 113 (1973).

93. *Casey*, 505 U.S. at 851.

94. *Lawrence*, 539 U.S. at 588 (Scalia, J., dissenting).

95. *See generally* Lochner v. New York, 198 U.S. 45 (1905).

was willing to translate expansively, but I think much of the reason that leads justices like Justice Scalia to be skeptical of *Roe* because of its potential for subjectivity and amorphousness might leave Brandeis to be skeptical of trying to push this substantive due process right to autonomy very far.

A final possibility for a liberty or autonomy based right would be to declare some sort of personal dignity that is protected in public. This is the path that Europe may very well go down. As you know, Europe protects dignitary rights far more expansively than we do. They're right now debating whether or not to codify a very expansive right called the "right to be forgotten" and you won't be surprised to learn that this right has its origin from French law, *le droit à l'oubli*, or the right of oblivion.[96] Americans all want to be remembered and the French want to experience oblivion. It's like something out of Sartre. That right has been proposed by the European Commission and is currently being debated.[97] If codified, it would allow any data subject to demand deletion of any data concerning him or herself—unless it's necessary in the judgment of a privacy commissioner for journalistic, scientific, or literary purposes. And if Google or Facebook or internet service providers fail to remove the data, they may be liable for up to one percent of their annual income, which, in Google's case last year, was forty billion dollars.[98] Now, Google has argued, with some merit, that this dignitary right as currently formulated is so expansive that it poses grave threats to American notions of free speech. It would allow me to demand that not only the removal of a photo that I post myself on Facebook and then I want to take down, but even to demand the deletion of that photo after it has been widely shared with others.

To see how dramatically that could threaten free speech, consider a recent case involving the right to be forgotten in Argentina.[99] An Argentinian pop star had posted racy pictures of herself and wanted them taken down even though they had gone viral. Yahoo in particular said it couldn't just remove the racy pictures. An Argentinian judge said the pictures had to come down or Yahoo would be fined a lot of money. So rather than remove the racy pictures, Yahoo deleted all mention of this woman from the Internet. If you plug her name, Virginia da Cunha, into Yahoo Argentina

96. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012).

97. *Id.*

98. *Id.* at 90-91; *see also Google 2012 Revenue Hits $50 Billion, Profits Up*, DAWN.COM, (Jan. 23, 2013, 1:14 PM), http://beta.dawn.com/news/780915/google-2012-revenue-hits-50-billion-profits-up.

99. Vinod Sreeharsha, *Google and Yahoo Win Appeal in Argentine Case*, N.Y. TIMES, Aug. 20, 2010, at B4, *available at* http://www.nytimes.com/2010/08/20/technology/internet/20google.html.

today, you get a blank page and a judicial order.[100] This just shows how dramatically this right to be forgotten would allow public figures to remove themselves from public discourse. And what if the pop star had wanted to run for parliament after posing for racy pictures as pop stars in Italy sometimes do? Should people really have the ability to selectively delete themselves from the Internet?

But the right to be forgotten sweeps even more broadly. There is a third category of information—not just pictures I post myself and are widely shared by others, but really any information about me that I think offends my dignitary right. So if you're tweeting or blogging this talk and saying that it's boring or clueless, after the talk, I could demand that this affront to my dignity be removed and it would ultimately be up to a European privacy commissioner to decide whether or not your tweet was in the journalistic or public literary interest. And it's really not the American tradition to give regulators and judges the power to make those substantive decisions when it comes to truthful and embarrassing information. In America, we believe that judges shouldn't tell citizens what they believe contributes to public discourse. So this is all to say that I don't imagine within the U.S. tradition we would declare a dignitary right that would give individuals these broad powers selectively to delete ourselves from the kind of archives that ubiquitous surveillance might create, but Europe might well go down that road. If it does, the clash between European notions of privacy and American notions of free speech may be dramatic. Brandeis, of course, was a champion of both values, but if forced to choose, my instinct is that he would favor democratic discourse over personal dignity.

So that's my proposal to you. It's not especially elaborate. But it attempts to be Brandeisian in the sense of beginning with the text of the Fourth Amendment, going on to identify the core value the Framers of the Fourth Amendment meant to protect, which was a degree of public anonymity for critics of the government, and then acknowledging what I think Brandeis would have considered obvious—namely, I am less secure in my person and electronic effects when those effects are aggregated and ubiquitously surveilled. Ubiquitous surveillance without a warrant is an unreasonable search of both my person and my electronic effects. It allows the government to invade my unexpressed thoughts, emotions, and sensations. Therefore, it is unjustifiable and unreasonable. By recognizing ubiquitous surveillance as an unreasonable search and seizure I think that Brandeis would have preserved our ability to maintain a degree of control over how our thoughts, emotions, and sensations are communicated to the government.

---

100. Search Results for "Virginia Da Cunha," YAHOO! ARGENTINA, http://ar.yahoo.com (search for "Virginia Da Cunha").

There are still undecided questions about the scope of this right. When does it kick in? Is it just month-long surveillance that violates the Fourth Amendment or day-long surveillance? Obviously, the problem is the volume of information, not the duration. One-day surveillance might be too much if it was done with a microphone, for example, or if a drone followed me around door to door, personally tracking me 24/7. That would be far more intrusive than the cops following me for a hundred miles, which the Supreme Court has said is okay.[101] We have to remember the substantive value we are protecting—namely, the amount of information about my sensations, thoughts, and emotions that is being collected against my will, not the amount of time during which the surveillance takes place. And obviously this involves line drawing decisions about how long particular surveillance technologies may be used and under what circumstances. It would be better for legislatures to draw these lines and there are bills pending in Congress that would limit the disclosure of geolocational information. Senator Leahy has included a provision in the ECPA reform bill and there is a bipartisan geolocational privacy bill cosponsored by Senator Ron Wyden, the Oregon Democrat, and Josh Chafetz, the Utah House Republican and Tea Party Libertarian who's been a fierce and admirable defender of privacy in the same way that Rand Paul was in his famous filibuster just a few weeks ago.[102] So although there is a bipartisan constituency limiting ubiquitous surveillance, I'm afraid it's not a majority constituency. The percentage of civil libertarians and libertarian liberals in the country at large have been estimated at about twenty percent[103] and so far the majorities in Congress have been unwilling to regulate these technologies, which is why the geolocational privacy bill doesn't seem to be going anywhere.

So although I would prefer a legislative solution and although the Court should be guided by the kind of limitations on geolocational surveillance adopted by certain states, I think in the end if we are to preserve in the twenty-first century the same amount of privacy that people took for granted in the eighteenth, the Court may have to act. If it acts modestly and cautiously, I think that Brandeis would have approved. He said in his right to privacy article that the application of an existing principle to a new state of facts is not judicial legislation: "It is not the application of an existing principle to new

101. *See* United States v. Knotts, 460 U.S. 276, 281-82 (1983) (holding that a person travelling on public roads has no reasonable expectation of privacy from the visual observation of police).

102. *See* Electronic Communication Privacy Act of 2013, S. 607, 113th Cong. (1st Sess. 2013).

103. David Kirby, *Poll Shows Romney Winning High Water Mark for Libertarian Vote*, CATO INSTITUTE (Sept. 27, 2012, 11:56 AM), http://www.cato.org/blog/poll-shows-romney-winning-high-water-mark-libertarian-vote.

cases, but the introduction of a new principle, which is properly termed judicial legislation."[104] So I think Brandeis would have endorsed this translation of an old principle in light of new technologies, and he provides an anchor for us to think about ways to do that. I'm always mindful of his challenge that "if we would guide by the light of reason, we must let our minds be bold."[105]

104. Warren & Brandeis, *supra* note 87, at 213 n.1.

105. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).