TINY CONSTABLES IN THE MOSAIC: MODERNIZING OVERSIGHT OF SURVEILLANCE IN THE AGE OF BIG DATA

*H. Bryan Cunningham**

Thank you for that generous introduction. I really appreciate being here. I think this is a great group and a great set of issues that the school's pulled together. I especially want to thank my good friend, your dean, John Farmer, for giving me the coveted after-lunch spot. I'll try to keep people awake if I can. I do have a little bit of bad news, though. I just wanted to let you know that now that I have the floor, inspired by Rand Paul's recent Senate filibuster,[1] I plan to hold it for thirteen hours or until I need to use the facilities, whichever may be earlier.

I mostly want to talk about developments in technology and judicial oversight, kind of the flip side of the coin that Jeff Rosen talked so eloquently about this morning.[2] But before getting to the

---

* H. Bryan Cunningham is a cyber security and privacy lawyer and Principal in the Los Angeles law firm of Bryan Cunningham Law, where he advises clients, including Fortune 500 companies, government, and multinational entities, on information security and data privacy and protection programs and other security-related issues. Cunningham is the principal author of legal and ethics chapters in multiple authoritative information security textbooks and has served in senior intelligence and law enforcement positions in the United States Government for Administrations of both political parties, most recently as Deputy Legal Adviser to then-National Security Advisor Condoleezza Rice. At the White House, Cunningham drafted significant portions of the National Strategy to Secure Cyberspace, the Homeland Security Act, executive orders on terrorism and intelligence, and other terrorism-related policy documents, and was one of the primary White House attorneys working with the 9/11 Commission. He also served six years in the Clinton Administration, as a senior CIA Officer and federal prosecutor. Cunningham was founding vice-chair of the American Bar Association Cybersecurity Privacy Task Force and was awarded the National Intelligence Medal of Achievement for his work on information issues. Cunningham has served on the National Academy of Sciences Committee on Biodefense Analysis and Countermeasures and as a member of the non-partisan Markle Foundation Task Force on National Security in the Information Age and the Bipartisan Policy Center's Cyber Security Task Force. He currently serves as a Senior Counselor to Palantir Technologies, and is a Senior Advisor for The Chertoff Group. Cunningham is licensed to practice law in California, Colorado, and the District of Columbia. Cunningham has no affiliation with Polaris Consulting, LLC.

1. *See* Catalina Camia, *Rand Paul Filibuster Ranks Among Senate's Longest*, USA TODAY (Mar. 7, 2013, 4:01 PM), http://www.usatoday.com/story/news/politics/2013/03/07/rand-paul-filibuster-longest-senate-thurmond/1970291/.

2. *See supra* Jeffrey Rosen, Keynote Address at the Rutgers Law Review

main topic, I've found, especially when talking to scholars of the post-9/11 generation, of which there are a lot here, that there are certain myths about electronic surveillance and government action that sometimes are helpful to dispel. I wanted to do a few of those first, right here in the beginning.

I have the text of a memorandum from the President to the Attorney General here.[3] I just want to read a couple of bits of it and then see who can guess who the President was that signed this. This is after a major electronic surveillance decision by the Supreme Court and this Attorney General recommended that certain wiretapping activity be shut down. The President says:

> I have agreed with the broad purpose of the Supreme Court decision relating to wiretapping in investigations. . . . [U]nder ordinary and normal circumstances wiretapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights.
>
> However, *I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.*
>
> . . . .
>
> You are, therefore, authorized and directed . . . to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of *persons suspected of subversive activities against the Government of the United States*.[4]

This was without limitation, without any warrant requirement, without really any substantive requirements at all except "subversive activities."

Who wants to guess the president?

Audience Member: John F. Kennedy?

You're on the right track.

Audience Member: Carter.

Nope, this was Franklin Delano Roosevelt.[5] Now you might say, "Well, of course, the most existential threat to the United States in the last hundred years was World War II. We were fighting the Germans and Japanese literally for our survival." Except this order

---

Symposium: Where There is No Darkness: Technology and the Future of Privacy (Mar. 29, 2013).

3. *See* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 279 (1976) (citing Confidential Memorandum from Franklin D. Roosevelt to the Attorney General (May 21, 1940)).

4. *Id.*

5. *Id.*

was signed in 1940—many, many months before Pearl Harbor.[6] So the notion that wiretapping started after September 11, 2001, or even was at its height after September 11, 2001, is something that I always like to just disabuse a little bit.

The other sort of bugaboo I just wanted to mention is the notion—which is particularly popular in Europe where I speak a lot but there's also a lot of misunderstanding here—that the Patriot Act[7] somehow created sweeping government authority that didn't exist before. In fact, many of the provisions of the Patriot Act were taking authorities that I had as a prosecutor in the Clinton administration and applying them to counterterrorism law enforcement and intelligence activities.

I want to give a big disclaimer here, first of all: I'm not here representing my client Palantir Technologies. And I'm not speaking on behalf of them, although I am proud to say that a couple of your presenters today are members of our Privacy Council, of which I'm the executive director. In fact, not all of the views I put to you today are even necessarily my own; they just are intended to promote discussion.

This morning Jeff Rosen did a great job of explaining how courts are viewing changes in technology and our understanding of our own expectation of privacy and how those dimensions interrelate. I want to talk about two other aspects of the same recent developments. One is how, at the same time that developments in technology are, in some ways, making the government more threatening to our privacy and changing our expectations of that privacy—and enabling both private sector actors and the government to surveil us and understand everything about us in a way that was perhaps envisioned by Justice Brandeis but by very few others until very recently—at the same time, I'm at least as worried that the traditional methods of judicial scrutiny and oversight of government surveillance are being eroded, and I'll talk a little about that. Finally, I hope to bring a little good news about how some of the same emerging technologies that are potentially increasing threats to our privacy and civil liberties also can help restore what I think has become an out-of-balance situation with regard to judicial oversight of government surveillance activities.

Jeff talked a lot about the recent U.S. Supreme Court decision *United States v. Jones*[8] this morning, so that'll save me a good twenty minutes, and he probably did a better job of it than I would have. But

6. *See id.*

7. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of U.S.C.).

8. 132 S. Ct. 945 (2012).

one of the aspects he didn't mention that I think is really important, if a little bit self-evident, is that the interaction of technology, privacy, and government surveillance had really gone off the radar screen, certainly of the U.S. Supreme Court and even of a lot of courts of appeal, for a long time, for decades really, prior to *Jones*. There were a few important cases here and there, but with *Jones*, I think that these issues are back on the front burner with a vengeance. And we've already seen what I think are the first few drips of a coming flood of appellate court and district court decisions trying to grapple with the implications of *Jones*, both reviving the property-based theory of privacy, which had been all but dormant since the *Katz* case in the late sixties, but also starting to introduce—at least in the views of Justices Alito and Sotomayor—what I think is an entirely new, at least at that level, concept of privacy analysis, which I'll talk about a little bit later.[9]

I'm not going to go back over this morning's ground in *Jones*, but I did want to briefly discuss this delightful fight in that decision between conservative bedfellows Justices Scalia and Alito.[10] I decided to do this talk for three reasons today. The first is, as I said, you have a fantastic dean who's a good friend of mine and he asked me. The second is that this is a really great set of topics. But really, the most important reason is that I couldn't resist giving a talk where I could work the phrase "tiny constables" into the title. And for those of you who don't know where that comes from, there's this great exchange in the opinions in *Jones* in which the two conservative Justices are trying to defend or attack the bringing of an eighteenth-century property concept of trespass into the twenty-first-century discussion of privacy. So to try and rebut Justice Alito's attack of the majority opinion's use of eighteenth-century tort and property law, Justice Scalia posits "a constable's concealing himself in the target's coach in order to track its movements,"[11] to which Justice Alito retorts, not to be deterred, that Scalia's eighteenth-century hypothetical requires "either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience."[12] Now, while I tend to be more of a believer in the gradual evolution of constitutional norms than I am a strict constructionist, I do think Justice Alito is being a little unfair here, albeit very funny. Surely, in

9. *See id.* at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring); Katz v. United States, 389 U.S. 347 (1967).

10. *See Jones*, 132 S. Ct. at 948; *id.* at 957 (Alito, J., concurring); *see also* Dahlia Lithwick, *Alito vs. Scalia: The Two Conservative Supreme Court Justices Brawl Over Technology and Privacy*, SLATE (Jan. 23, 2012, 6:38 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2012/01/u_s_v_jones_supreme_court_justices_alito_and_scalia_brawl_over_technology_and_privacy_.html.

11. *Jones*, 132 S. Ct. at 950 n.3.

12. *Id.* at 958 n.3 (Alito, J., concurring).

colonial times, agents of the Crown paid informants to surreptitiously listen in on conversations of individuals and otherwise surveil them without their knowledge or consent.

Since I can't begin to compete with Jeff's discussion of what courts or Congress may come to protect as substantive privacy interests in the coming decades, I want to focus instead on something I think is at least as important and that is how the courts are going to be able to protect whatever they determine to be our substantive privacy rights. In this regard, I think there's some fairly bad news recently for privacy champions, at least in the short term, sort of a two-pronged attack—perhaps unintentional but an attack nonetheless—on the ability of the judicial branch to conduct meaningful oversight.

The first recent challenge to traditional judicial oversight is straightforward and I suppose intentional or at least knowing, and that is what appears to be a fairly significant erosion of the ability of courts to take meaningful jurisdiction of national security surveillance cases.

A recent Supreme Court decision, unfortunately again five to four, called *Clapper* —who is the Director of National Intelligence—*v. Amnesty International*, is illustrative.[13] In that case, the ACLU and Amnesty International and others had brought suit challenging the constitutionality of recent amendments to the Foreign Intelligence Surveillance Act, which, of course, is the primary statute under which U.S. government electronic surveillance (for foreign intelligence, not law enforcement purposes) is conducted.[14] The ACLU and Amnesty International brought together a number of journalists and activists and lawyers who took the position that they had standing to challenge the government's interception, even though they had no knowledge of whether they had actually been intercepted, because it was reasonable to assume that they had been, since many of them dealt with suspected terrorists and others overseas whom they surmised the government would want to surveil, and also because they argued there was no meaningful way for a potential plaintiff who actually was being surveilled to know that and, therefore, no way to bring a constitutional challenge to the statute before the court.[15] The ACLU and Amnesty International basically argued that if Americans' privacy rights were going to be vindicated at all, courts should permit more relaxed standing

13. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

14. *See id*. at 1142-43; Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008) (codified as amended in scattered sections of 50 U.S.C. (Supp. I 2008)) [hereinafter FISA Amendments Act].

15. *Clapper*, 133 S. Ct. at 1151-52.

requirements than courts had done in the past.[16]

The Court held, five to four, on exactly the lines you would think they did, that the plaintiffs did not meet applicable standing requirements because they were not able to show they had been or actually were being surveilled.[17] Of course, the problem with that analysis is how would they know if they were being actually surveilled? In a few of the Bush-era wiretapping cases, some courts had left open a little window that you might be able to achieve standing even if you couldn't show any actual injury.[18] But I suspect that in the wake of this case, those doors are going to be closed. I'll read you the ACLU's commentary when this decision was handed down: "It's a disturbing decision. The FISA Amendments Act is a sweeping surveillance statute with far-reaching implications for Americans' privacy. This ruling insulates the statute from meaningful judicial review and leaves Americans' privacy rights to the mercy of the political branches."[19]

Just as an aside, I think there is a rather interesting interplay with the discussion we had this morning about what sorts of things should be left to the political branches and what sorts of things should be left to the judiciary. Though I think the ACLU analysis was a bit overwrought, it is becoming increasingly hard, for me at least, to see how any plaintiffs will have standing to sue for foreign intelligence surveillance that is never used in a criminal prosecution. In a criminal prosecution, defendants may get some access to, and ability to challenge the use of, FISA-collected information, particularly if such information is to be used against them.[20] And under recent amendments to FISA, electronic communication service providers receiving certain types of FISA orders can file a petition with the Foreign Intelligence Surveillance Court challenging such orders.[21]

But we've seen in terrorism cases and, increasingly, in cyber security cases that prosecution is not always the preferred method of dealing with such threats. Even though President Obama came into office promising to revert to the pre-9/11 way of dealing with terrorism to some degree, there still have not been many high-profile cases brought in the criminal courts. And although I think they're trying to get back to that, cyber cases, in many instances going

16. *See id.* at 1155-56.

17. *See id.* at 1142, 1155.

18. *See, e.g.*, Jewel v. NSA, 673 F.3d 902, 910-11 (9th Cir. 2011) (finding that plaintiff has standing to challenge warrantless telephone surveillance).

19. *Supreme Court Dismisses ACLU's Challenge to NSA Warrantless Wiretapping Law*, ACLU (Feb. 26, 2013), http://www.aclu.org/national-security/supreme-court-dismisses-aclus-challenge-nsa-warrantless-wiretapping-law.

20. *See* FISA Amendments Act, 50 U.S.C. § 1806(e).

21. *See id.* § 1803(a).

forward, I think, are just going to be impossible to be dealt with in a domestic American criminal court.

I think that what's overwrought about the ACLU's response is that there's not, as it suggests, no avenue to challenge foreign intelligence surveillance. The Foreign Intelligence Surveillance Act itself provides for a court of review, a federal appellate court, above the Foreign Intelligence Surveillance Court that actually issues the surveillance orders.[22] First of all, in recent years, this appellate court has actually met and issued opinions, which they didn't do for the first twenty-some years of existence. But it also took the step of inviting the ACLU and the National Association of Criminal Defense Lawyers to come in and represent the antigovernment side, even though they conceded that no one actually had standing to argue on behalf of intercepted plaintiffs.[23] And then, of course, due to some of the amendments in the last few years, telecommunications service providers who are served with an interception order signed by the FISA court that they believe is unconstitutional do have the ability to go to the lower FISA court and the court of review, the appellate court, and challenge those orders.[24] That's been done at least once and, unlike the lower FISA court, the court of review has consistently published versions of their decisions, albeit heavily redacted.[25] So, at least there's a little bit of ability for the public to actually understand what goes on there.[26] But, by and large, the ability of Americans to challenge government intelligence surveillance is getting more difficult due not only to the standing issues, but also because the types of threats that are coming down the pike, or perhaps are already here, are going to require a change in the way the judiciary conducts oversight if it is to be able to meaningfully do so going forward.

For example, as there often is, there is a major article in today's *New York Times* about cyberattacks.[27] Specifically, while in the past many of those types of attacks have been theft of intellectual property, espionage attacks—kind of nuisance attacks—such attacks

22. *See id.* § 1803(b).

23. *In re* Sealed Case, 310 F.3d 717, 719 (FISA Ct. Rev. 2008).

24. *See* FISA Amendments Act § 1881a(h)(4).

25. *See, e.g.*, *In re* Directives, 551 F.3d 1004 (FISA Ct. Rev. 2008).

26. Several months following these remarks, multiple Foreign Intelligence Surveillance Court orders were declassified and publicly released. *See* James R. Clapper, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)*, OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE (Sept. 10, 2013), http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document?tmpl=component&format=pdf.

27. Nicole Perlroth & David E. Sanger, *Cyberattacks Seem Meant to Destroy, Not Just Disrupt*, N.Y. TIMES, March 29, 2013, at B1.

are becoming deliberately more destructive.[28] And Wednesday, on his way to hear one of the DOMA cases, Justice Roberts discovered at a Starbucks in Maryland that his identity had been stolen and his credit cards had been shut down as a result.[29] So he had to hear the first couple hours of DOMA without his Starbucks caffeine, which in and of itself is not a threat to national security, but as more very senior officials in the judiciary and executive branches and in Congress see themselves as targets of some foreign cyberattacks, we may see a lot more sweeping action to empower the government even more to combat them.

Secondly, with regard to recent threats, or at least inevitable changes, to the nature of judicial oversight of government surveillance, the nature of cyberattacks today and going forward is that they happen so fast and at such volume that the ability to determine who your attackers are, what their purposes are, and, importantly, where they are, is so difficult in real time that I believe that, if it hasn't happened already, the government soon will seek, and get, additional surveillance authorities and exercise them in such a way that the traditional methods of judicial oversight—the issuing of individual warrants or orders based on particularity in advance—unfortunately is just not going to be sustainable, at least for these kind of national security threats.[30]

So where do we go from here in terms of judicial oversight, which I, at least, think needs to be restored and retooled for the twenty-first century? Back to the tiny constables. In the American colonial experience, a constable was typically a law enforcement officer, and obviously that's the sense in which Justices Alito and Scalia were using the term.[31] But, whenever I have to come and speak to a room of esteemed law professors, I always try to do a little English history research just so I can sound like I know what I'm talking about. And it turns out that, in thirteenth-century England, according to the jurist Henry de Bracton, the role of the constable was as the eyes and

---

28. *See id.*

29. Al Kamen, *Chief Justice Hit by Credit-Card Fraud*, WASH. POST (Mar. 28, 2013, 2:53 PM), http://www.washingtonpost.com/blogs/in-the-loop/post/chief-justice-hit-by-credit-card-fraud/2013/03/28/63a9bf06-97d4-11e2-814b-063623d80a60_blog.html.

30. These remarks were made on March 29, 2013, several months before revelations of secret National Security Agency and FBI surveillance programs apparently operating under classified "programmatic" orders, rather than individualized judicial warrants. *See* Barton Gellman & Laura Poitras, *U.S. Mines Internet Firms' Data, Documents Show*, WASH. POST, June 7, 2013, at A01. Subsequently declassified FISC orders confirmed this as well. *See supra* note 20.

31. *See The Early Days of American Law Enforcement*, NAT'L LAW ENFORCEMENT MUSEUM INSIDER (Apr. 2012), http://www.nleomf.org/museum/news/newsletters/online-insider/2012/April-2012/early-days-american-law-enforcement-april-2012.html (explaining the role of constables in colonial times); *see also supra* notes 9-10 and accompanying text.

ears of the court, finding evidence and recording facts on which judges could make a ruling.[32] And that's the sense that I'm suggesting we think, for a moment, about tiny constables because I believe that the eyes and ears of the court and the judicial oversight function can be meaningfully enhanced through the use of technology, tiny electronic eyes and ears of the court for the twenty-first century.

The Foreign Intelligence Surveillance Court of Review, in its 2008 opinion refusing to strike down on constitutional grounds provisions of the Foreign Intelligence Amendments Act, said that, even in the absence of the traditional protections of the warrant requirement, the government can produce and the judiciary can approve—if they find them reasonable—"plausible proxies for the omitted [traditional Fourth Amendment warrant privacy] protections."[33] I believe that going forward technology is going to have to be a major component of those "plausible proxies" for traditional judicial oversight.

The good news is that there is becoming available now technology—full disclosure: including by the company I represent, among others—which can do things like strictly enforce judicial rules for government data collection, data access, data analysis, data sharing, and duration of availability of acquired data. So even in the situation where government has collected information—that is, they've acquired it, perhaps without individualized judicial warrants—I believe there is the ability for, and still the possibility of, robust judicial oversight over who it's shared with, who gets to access it, how much analysis may be done on it, including with technological capabilities like automatic destruction and deletion, automatic minimization of information not pertinent to the judicially authorized investigation, and the like.

In addition, we now have capabilities to provide comprehensive, tamperproof, and easy-to-use audit logs to facilitate oversight and review. So a judge might issue a forty-five day order for acquisition of information but with very specific targeting limitations, i.e., what subset of the information may be seen and used by human government agents. The judge, through his tiny technological constables crawling through the bits and bytes of the government's data systems, could get detailed, very specific periodic reports on exactly who's being surveilled, where the false positives are, where the false negatives are, and, most broadly and importantly, is the government following the rules and restrictions that the court's

---

32. *See* 4 HENRY DE BRACTON, ON THE LAWS AND CUSTOMS OF ENGLAND 136-37 (George E. Woodbine ed., Samuel E. Thorne trans., Belknap Press rev. ed. 1977) (1569).

33. *In re* Directives, 551 F.3d 1004, 1013 (FISA Ct. Rev. 2008).

programmatic approval required?

Also, of course, robust auditing deters misuse of the system and helps to identify abuse that inadvertently or intentionally happens.

And finally, on the topic of auditing, the kind of reports that can now be generated using technology can be easily sanitized and declassified for purposes of reporting to the judiciary, to Congress, to the media, and to the American people. We can now do very precise analytics of the authorized collection, analysis, and use of data to determine the magnitude of incidental overcollection, collection of information that wasn't approved for targeting that's happened, and then finally, as I mentioned, the enforcement of durational, subject matter, and other limits on what's allowed to be collected, accessed, used, and stored.

Now let me leave you with one other thought on the mosaic concept. I have some Department of Justice rules on mosaic in your materials. I think the combination of what Justices Alito and Sotomayor were suggesting in the *Jones* case may well lead, eventually, to a largely new area of judicial oversight of government surveillance and use of collected information. Traditionally, almost all of our judicial controls have been put on collection. Once the government has information on you, with some exceptions like the minimization rules under FISA,[34] there typically has been very little scrutiny or control over how that data is actually analyzed and used. But I find, in the opinions of Justices Alito and Sotomayor in the *Jones* case, a hint that, at some point, the Court might find that, even if each individual piece of information about you is collected lawfully by government, the power and the ability now of the government to use technology to analyze such data and to come up with a 24/7 dossier of what you're doing, even if that's not through GPS collection, as in *Jones*,[35] even if they're only pulling together toll-road-use data or other things that are seemingly less privacy invasive, that kind of analytical activity may at some point raise implications for the Fourth Amendment to the point where the judiciary may want to scrutinize that.

When I was a young CIA attorney in the early years of Clinton's administration, I frequently had to litigate something called the Mosaic Theory. And I put in the materials the DOJ guidelines for that under the Freedom of Information Act.[36] In that context, we were using the Mosaic Theory to assert that—and all the other intelligence agencies did it as well—even where a particular piece of information by itself is unclassified and not damaging to the national

---

34. *See* FISA Amendments Act § 1801(h).

35. *See* United States v. Jones, 132 S. Ct. 945, 948 (2012).

36. *See* U.S. DEP'T OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT 170-71 (2009), *available at* www.justice.gov/oip/foia_guide09/exemption1.pdf.

security if disclosed, if you put enough of those unclassified bits of data together and you're sufficiently expert at understanding them, it could, as a whole picture, a whole mosaic, if you will, add up to data that could be properly classified and protected by the U.S. government. And, Justices Alito and Sotomayor, following the D.C. Circuit decision below,[37] seem to be, brilliantly in my view, taking that basic argument, for years used as a shield by the government against disclosure of information, and turning it into, if you want to torture the metaphor, a sword for privacy.[38] And what I think they may be saying or they may get around to saying is even though particular government intrusions individually may not implicate the Fourth Amendment, when enough of them are put together, on the collection side, which is explicitly what *Jones* deals with,[39] but also on the analysis and use side, there may be a resultant need for judicial scrutiny under the Fourth Amendment. And here, again, I think the good news is that, with properly deployed and used technology, there can be a much better ability than in the past to actually track everything the government's doing with data: what they're pulling together, what they're connecting, what they're distributing, and to better be able to understand where the line might be crossed requiring a warrant or other Fourth Amendment protections.

Not even Jeff Rosen this morning could predict where those lines might be drawn by our courts in the future, so I'm certainly not going to try to predict that. But I do think that, sooner or later, they will be drawn.

Thank you.

---

37. United States v. Jones, 451 F. Supp. 2d 71, 90 (D.D.C. 2006).
38. *See id.* at 88.
39. *Jones*, 132 S. Ct. at 949-54.