Idaho Law Review

Volume 51 | Number 3 Article 7

March 2019

Transcript of Keynote Speech

David Medine

TRANSCRIPT OF KEYNOTE SPEECH

David Medine

I guess I'm the first speaker to have to give a disclaimer, which is that my views today don't necessarily represent the views of the Privacy and Civil Liberties Oversight Board or any of its other members. I want to talk a little bit about our board and following up with from what Annemarie [Bridy] said of how we got started and then turn to some topics for today.

After the 9/11 attacks, as I think you may know, a commission was formed to address what happened and how we can do a better job in protecting our country against terrorist attacks. And if you haven't read their report I highly commend it.[1] It's extremely readable, but a very detailed account of the problems that led to the attacks on 9/11 not being thwarted. At the end of this, roughly, 500-page report there's about two or three paragraphs that say, by the way, let's not go too far in the direction—so far in the direction of protecting national security that we compromise privacy and civil liberties. Because what makes us a great country is the fact that we have both privacy and civil liberties and national security. And actually having both of these are strong values that complement each other and don't contradict each other.

And so the 9/11 commission recommended the creation of a board to advise the government on how to strike that balance. So shortly after that, a board was created in the White House called the Privacy and Civil Liberties Oversight Board and it started its work. But the White House felt that it could edit the board's work because it was in the White House. And so one of the board members resigned in protest, Lanny Davis, and said that the board was not sufficiently independent to exercise oversight of federal counterterrorism programs.

Congress agreed and abolished PCLOB 1.0. In 2007, Congress created PCLOB 2.0 as an independent agency in the executive branch, which is a bit of a non sequitur, but ends up working out pretty well for us. We're in the executive branch, and that's a real plus, because we have access to deliberative materials in the executive branch that, say, Congress or the courts might not get access to, privileged information, classified information. Every member of the Board and every member of our staff has to have the highest level of security clearance. So that's, I think, one of the pluses of being in the executive branch, but it's also a plus being independent because it gives us credibility and allows us to look at programs and express our own views.

And so, for instance, on the 215 program, which I'll talk about briefly later, our Board concluded that the program was not legal and also bad policy, but the White House disagreed with our conclusion about the legality of the program. We don't have to clear our views through the White House or the Office of Management and Budget, we can simply express ourselves by a vote of the board. And so I think that hopefully will give us credibility in both the national and the international context to say that we can take a look at programs, sometimes they're classified so we may not be able to discuss them in public, but knowing that we are giving a serious independent view of how those programs operate I think is really critical.

1. National Commission on Terrorist Attacks upon the United States, the 9/11 Commission Report (2004).

So again in 2007, legislation was created authorizing PCLOB 2.0. It took President Obama a while to get a slate of nominees together.

I noticed there's a Whole Foods across the street—and my story begins at Whole Foods as well. I was shopping at Whole Foods in September 2011, and I got a call from Peter Swire, who some of you may know, saying the White House is looking for people to chair PCLOB. "Would you be interested?"

And my first reaction is, "What's PCLOB?" And he explained it and I looked it up and I said, "Sure. I'd be happy to put my name in the ring." That was in September 2011—and after countless paperwork and background checks and interviews, finally, on December 2011 President Obama nominated me and two others to be on the Board, having previously nominated two other people, so we had a full slate of five. As Annemarie mentioned we have five members on our board, no more than three of any one political party, so we currently have three Democrats, two Republicans and we serve staggered six-year terms.

I thought the big hurdle was getting nominated and so in December 2011 I thought it'd be pretty smooth sailing after that. It turns out it took the Senate 510 days to act on and vote and confirm me as chairman of this board.

The Senate may have had some wisdom there because I started on the board on a Monday, we had no office, we had no permanent staff, two detailees, we had no website and no email system, that was on Monday. On Thursday the Snowden leaks occurred.

So the question was: Are we going to be relevant or are we irrelevant? And I thought it'd be better to be relevant. So, on Friday, I wrote a letter to the attorney general and to the Director of National Intelligence saying that we would like to be briefed on the two programs that Snowden initially leaked, the 215 and 702 programs, and p.s., I don't have a security clearance.

On Monday I had a security clearance. On Tuesday we were briefed at the Justice Department by the NSA, FBI, and DOJ and so forth on how these programs operated. And then about two weeks after that we met with the President in the Situation Room to discuss surveillance issues. So it was quite a busy couple of weeks on the job, and it's been quite a busy year and a half or so on the job as well.

Since then, as I think as you may know, we've issued two reports and we've embarked on an additional project, as well as some smaller things. But in looking at the agenda for today on [private and public] surveillance, my former life with the FTC would have been from the private sector side, and my current job is focused on the government side. And so—I think that naturally brings to mind the Fourth Amendment.

I really want to focus today on the Fourth Amendment's application in this context, particularly government surveillance. And I wanted to give you three aspects of it. Two of them relate to my work at PCLOB and another relates to some pro bono work I've done for the Constitution Project in the past on video surveillance in public places. The three aspects of the Fourth Amendment I wanted to discuss are, basically, narrowing aspects of the protections it provides: [1] the reasonable expectation of privacy standard, [2] the third party doctrine and [3] the foreign intelligence exception. The first two have already been touched on previously today.

But I think, as people know, the Fourth Amendment requires a warrant in most cases. The protections of the Fourth Amendment prior to the famous *Katz*

decision[2] focused on the home, which was the subject of the first panel. And then after *Katz*, it focused more on people than places which, in some ways, expands on the second panel in terms of people out and about, and not just in their home, getting protection under the Fourth Amendment.

And the standard that was enunciated is that there be a reasonable expectation of privacy in terms of when the Fourth Amendment would apply. The *Katz* case looked at wiretapping one phone booth and listening in on one person's conversations. The standard was developed at a time before the government had the powers we've heard about today that are sometimes used by for pervasive surveillance. The government uses video cameras, license plate readers, sometimes GPS. And these tools allow for more than a snapshot, or for those students in the room, Snapchat, of people's lives and how they operate. And these inputs from a variety of devices as mentioned before can be linked together and merged using facial recognition, as Yana [Welinder] mentioned, and other devices to create a profile of someone, a near complete picture of what they do every day and all day.

The question is: is there a reasonable expectation of privacy in collecting all this information about people that creates a very detailed profile about people's lives, what they do, who they meet with, what they talk about. Under the *Katz* expectation of privacy, if you have a video surveillance camera on the wall and a sign underneath it that says, "CCTV Monitoring Here" or "This area is being surveilled," one could argue that negates any expectation of privacy and, so therefore, the Fourth Amendment would not apply to that type of collection activity.

One could also argue that when you drive on the road, you know that you're in public and don't have an expectation of privacy. And so when a license plate reader picks up your car and knows where you've gone all throughout the city, you're acting in public and therefore, also didn't expect to be private.

I guess another thing I should mention is policemen. We think of it as being appropriate for police to tail people— [we think of this] as permissible. But what if we assigned a policeman to, say, a dissident, and they tail him day after day after day, night after night? At some point you reach the point—even if you're operating in public—where it tips the balance and you're gathering so much information about someone over such a long period of time that it should be considered a search under the Fourth Amendment.

We also now have publically available information, Facebook, Twitter, all kinds of social media that give not only what people do, but oftentimes their location. And so we can, again, map where they've been throughout the day. You post your picture on Facebook—that indicates where the picture is taken. And again [if] people don't use privacy settings, [the government] can gather that information together and create a very detailed profile of how its citizens are operating.

Now, some have argued that there isn't an expectation of privacy that the government will create these detailed profiles of you throughout your day; but I'm not sure that the courts are going to recognize that as a limiting factor on government surveillance activities. So I don't think that the expectation of privacy standard is really appropriate as we move forward into a new generation where we can live our lives virtually and in the cloud. This is one area where the Fourth Amendment, I think, could benefit from some changes and interpretation to adopt a more

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

substantive standard of protection. Not looking at the individual's view of whether the government is invading their privacy, but looking at the nature of the government's activity collectively and decide, essentially, has that crossed a line. [A standard] where notice of surveillance is not enough, if you're being surveilled in the Panopticon [as referenced earlier by Jeffrey Vagle] or wherever it happens to be. At some point, the government should be limited in its powers to surveil citizens.

The second area I wanted to talk about is the third party doctrine which is, to some extent an element of the reasonable expectation of privacy standard. [This doctrine states that] if you give your information to a company, you can't reasonably expect that that information is supposed to be kept private. Margot Kaminski made a stunning comment earlier today, which is that, at least to some extent, the way the law is developing now, citizens have more protection against companies' surveillance activities, under consumer protection law, than they may have under the Fourth Amendment when the government surveils their activities. And if that's true, I think that's a somewhat troubling development in terms of the power balance between citizens and the government.

But I want to talk a little bit about how our Board came to bump up against the third party doctrine. This happened with one of the first programs that we looked at: the Section 215 telephony metadata program. And for those who may not be aware of it, it's a program in which the NSA goes to phone companies and gathers information, not about the contents of your phone calls, but the metadata, which is the number that your phone number dialed, whether the call connected, how long the call lasted, and some basic information like that. And they gather all that information into a massive database. The purpose of that is, say, you find a terrorist in a cave in Afghanistan who called someone in the United States, that is certainly potentially interesting. If someone from Al-Qaeda is calling someone in Cincinnati, you might want to know if there's a terrorist plot underway and maybe someone has been planted in Cincinnati or there's some cooperative person in the United States that's helping out Al-Qaeda.

So what the government can do under this program is not only see that call coming in, but then find out who the person in Cincinnati called on the theory that maybe they're in on a terrorist plot and the government can find who the co-conspirators were. And then [the government can] go out another level to see who those people, every one of those people, called and everyone who those people called. So it's a growing number of steps that are taken in terms of understanding—of reaching out to see if there's a terrorist plot underway. We looked at the program from three perspectives. One, is it legal? Two, is it constitutional? And the third is, on policy grounds: does it strike the right balance between privacy and civil liberties and national security?

On the legal side we concluded that the program did not fall properly under the statute for a number of reasons. One is that the statute says . . . that if the government wants to collect this type of information it has to be relevant to an investigation.[3] And the question is: How could the collection of every American's phone records be relevant to any investigation and have "relevance" have any meaning? And so in our view, that statute and the program did not match up.

3. *See* 50 U.S.C. § 1861(b)(2) (2006).

In addition just as a somewhat technical matter, the Electronic Communications Privacy Act[4] restricts phone companies' ability to provide metadata to the government, and it provides specific programs under which that data can be provided; Section 215 is not one of those programs. And so the statute doesn't match there as well.

Just a third example is the statute says that the FBI shall collect this information. And as we know, the NSA collects the information; not a totally trivial difference. The FBI is a domestic law enforcement agency and we're looking at potentially domestic crimes. The NSA, obviously, has a more international focus. So for a number of reasons the board concluded the program didn't match up with its statute.

On the policy side—and Jennifer Lynch talked about this earlier, about some of the privacy implications of having a map of your phone calls and who you're interacting with—just the mere fact that the government is collecting information about your phone calls has the real potential to chill freedom of association, freedom of speech, and freedom of religion. Just think of someone who's a whistleblower who wants to call a reporter at a newspaper knowing that the government knows about that call. Or some of the more typical examples: you call an oncologist and the next call is to a funeral home, I think you have a pretty good sense, unfortunately, of what's going on. And there are lots more examples: of religious groups meeting together, political groups meeting together, etc.

So the mere fact that the government is collecting this information raises some significant civil liberties issues and privacy issues. But our job is not to look at just the privacy and civil liberties side of the equation, it's also to look at the national security side. And so as many of you may know, right after the Snowden leaks, the government advanced a number of success stories under which 215 was asserted to be successful. So we were able to go to the government – and there were about a dozen of those ultimately—and get the files on each of those cases, some of which included classified information, and see what role the 215 played in the asserted success in each of those cases.

We looked at a number of metrics: catching co-conspirators, evidence of other crimes, and also thwarting terrorists' plots and identifying co-conspirators. And we concluded, based on all of those metrics, that the program was not effective. It had certainly not thwarted any terrorist plots, but it also had been of limited efficacy in those other areas. And we also found that what limited efficacy it had, could have been achieved through other legal resources, like national security letters or grand jury subpoenas. The most typical case that was mentioned was the Zazi case where someone from Colorado came to bomb the New York City subway. That was asserted to be a 215 success story. But 215 didn't come into play until Mr. Zazi stopped, realized they were onto him, left New York, went back to Colorado, was arrested in Colorado and they picked up, through 215, one of his co-conspirators. [The 215 program] had nothing to do with thwarting the plot and bombing the subway in New York.

Just on a policy ground the board said, that based on various significant privacy and civil liberties concerns, [the program was] not effective on the national security side, and recommended that the program be discontinued in its current

4. 18 U.S.C. § 2510 (2006).

form. And instead that the government [should] go on a case-by-case basis to phone companies when they have a particular need for phone information and get the records from the phone companies instead of having the bulk collection. We essentially did not accept the argument that you can't find the needle in a haystack unless you have the haystack. There are other ways of finding needles that are more privacy and civil liberties protective than having the government hold all this transactional information.

So then the third part of our analysis was constitutional. And the question is: Did this collection of information on Americans run again afoul on the Fourth Amendment? It certainly seems very troubling that the government -- without a warrant -- is gathering massive amounts of information with no suspicion about any individual. But what we quickly found is there is this *Smith v. Maryland* case.[5]

And I want to just briefly tell you some of the facts of *the Smith v. Maryland* case on which the NSA's collection of millions of phone records is based. [In *Smith,*] a woman in Baltimore was robbed and the robber then proceeded to call her and harass her on the phone. As a matter of fact, one day he even called her and said if you just look outside I'll be outside your door in my car. And so she looked out and there was this Monte Carlo driving by. She reported it to the police that this robber was driving around and harassing her. The police put out a lookout for this particular car with this particular person's description. And on March 16th of that year, someone identified that car and that person.

The police went to the phone company and put a pen trap on his phone, which, basically, is a primitive device that would allow [them to collect] what numbers he was calling out to. Not nearly as sophisticated as what the NSA does in terms of its telephony metadata program of seeing if the phone call was connected and how long it lasted; [the pen register] simply [collected] what calls were made. That was on March 16th. On March 17th, they found him calling her number. Bingo! They got what they wanted one day later. And on the basis of that, they got a search warrant, searched his home, found he had put a fold on the page of his phone directory that had her number on it, and arrested him and prosecuted him.

He was convicted. And he went to the Supreme Court and argued that the search warrant was based on information that was collected [in violation] of the Fourth Amendment and the search was unconstitutional. His case went to the Supreme Court and the Supreme Court said no, you give your phone records to the phone company when you make a phone call, and you know that. And so, therefore, when the police put the pen trap on your phone and got the information it wasn't really private— [it was] public in the sense of giving it to the phone company and not keeping it private. And so, therefore, the pen trap search of your phone records was constitutional and didn't violate the Fourth Amendment.

Just as a side note, we invited in the lawyer who argued the case for Maryland who won. He said he tried to make it as narrow of a case as possible. And he said he's horrified that his little decision in this Baltimore . . . robbery case has now become the foundation for an NSA collection program; but sure enough, it has been. And the question is: Should it be?

I should say what we concluded was that the government was reasonable in relying on *Smith v. Maryland* as the basis for this program because at least up until

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

now, *Smith v. Maryland* is good law and the third party doctrine which allows the government to collect this information is still viable.

But the question is, as we go forward as cases are working their way up through the system, one judge has held the program unconstitutional, some have held it constitutional: Should the Fourth Amendment restrict this kind of government collection?

There are some important distinctions between the 215 program and the *Smith v. Maryland* case. One is, obviously, everyone's records are being collected. In *Smith*, [collection] was for a few days, but the 215 program goes on for months and years. In *Smith*, there was suspicion about this particular person. Hopefully, not all of us are suspect in an investigation of the government, and yet [under 215] all of that information is being collected. And so it's really quite an extension of *Smith* . . . admittedly it probably has to work its way to the Supreme Court to have changes made to the third party doctrine.

The same principle has been found in other cases in other contexts in the Supreme Court. There's the *Miller* case,[6] where records also fell under the third party doctrine and weren't protected under the Fourth Amendment. In response, Congress passed the Right to Financial Privacy Act that protected financial records.[7] But the same principles apply to credit card records, online shopping, library records— all held by third parties.

As was mentioned earlier, there's some language in the *Jones* case in the Supreme Court that suggests that maybe five of the justices are willing to revisit these issues.[8] Justice Alito, concurring in that case, contrasted the short-term monitoring that might have occurred in prior cases, to the longer term collection of information with the GPS tracking device, [arguing] that's something that might tip the balance.[9] Justice Sotomayor suggested that there might be a need to reevaluate the third party doctrine given the reasonableness of how much information was being collected.[10]

So I guess my view is that the third party doctrine should either be abandoned or sufficiently narrowed, so that it doesn't allow massive bulk collection of information by the government on citizens everyday on constitutionally-protected activities. I think it's appropriate the Fourth Amendment has evolved from one's home, to expectations of privacy, to people's virtual existence now, and it should recognize that we live our lives in the cloud and online. Merely the fact that a third party company is handling our information should not take it out of the protections of the Fourth Amendment with regard to the government's collection activities.

And the third potential narrowing of the Fourth Amendment I wanted to mention is the foreign intelligence exception. According to the Supreme Court, warrantless searches are *per se* unreasonable, except in well delineated exceptions. And the Court left open, in a case many, many decades ago, whether there might be an exception for national security or the activities of foreign powers. The lower courts that have considered the question of whether there's a foreign intelligence exception to the Fourth Amendment have generally found that there is one. Although, it's

6. United States v. Miller, 425 U.S. 435 (1976).
7. 2 U.S.C. § 3401 (2006).
8. United States v. Jones, 132 S. Ct. 945 (2012).
9. *Id.* at 964 (Alito, J. concurring).
10. *Id.* at 967(Sotomayor, J., concurring).

yet to make it up to the Supreme Court. Even the Foreign Intelligence Surveillance Court has indicated that the surveillance directed at a foreign power, or agent of a foreign power, would be exempt from the Fourth Amendment. But it's worth noting that U.S. citizens or U.S. persons can be agents of a foreign power, and so what that exception would allow surveillance of U.S. persons without a warrant. So I think it's something important to consider.

We came up against this in the 702 program, which was the other program that Snowden leaked back in in 2013. It's a targeted program; it's not a bulk connection program. Under 702, the government targets accounts that belong to people who are not Americans, who are overseas and where there's a foreign intelligence purpose. But unlike the 215 program, it's actually collecting the contents of emails and the contents of phone calls. The government has to go to court to approve this overall program, but does not have to go to court and get approval for each individual email account that's been targeted.

And so the first question is: Why does this impact the Fourth Amendment at all? And the answer is: Even though you're collecting communications of non-U.S. persons overseas, occasionally those people talk to or email with Americans. And so the government is collecting a database of contents of communications and phone calls of Americans even though their targets may have been non-U.S. persons.

And so the question is: How does the Fourth Amendment apply in this context? For the purposes of our 702 report, we assumed without deciding that there was a foreign intelligence exception. And what that meant is that there was not a warrant requirement in this case. Now, I think that that's something that certainly the courts could, and may well, revisit as there are also challenges underway to the 702 program. But, even without a warrant, that's not the end of the story under the Fourth Amendment. Even a warrantless search has to be reasonable under the Fourth Amendment. And one of the things we looked at in this program was whether the protections on the way the program operates in targeting and oversight and so forth were reasonable. Our conclusion as a board is that this program went, essentially, right up to the line of reasonableness, but the Board was not prepared to say the program was unreasonable under the Fourth Amendment.

However, one of my fellow board members, a former federal appellate judge, Patricia Wald, and I dissented from the Board's report and argued that, at least in one context, there should be court approval for searches. [There is a] big database now of communications, collected on foreign targets that the U.S. government can search for U.S. persons. Basically, it can gather my communications with folks overseas over a period of time and with different people, and compile those, looking at me and my communications.

Judge Wald's view and my view was that that this type of collection on U.S. persons at least requires court approval, whether it's in the national security context by NSA, or in the law enforcement context by FBI. This information wasn't gathered with a warrant and even if that's acceptable, this is a use of the information, now shifting the focus to Americans, that at least in our view ought to trigger the protections of a federal judge approving the collection.

So going forward, the foreign intelligence exception is another area where we could really benefit from some court guidance on whether, first of all, an exception

exists at all, because we have not gotten any expression from the Supreme Court [in that area]. And if it exists, what are the contours of that exception?

Our Board has now shifted our focus from the 215 and 702 programs, which were the initially leaked programs, to the Executive Order 12333[11] which is not a program, it's an authority. It's something that President Regan issued to govern the entire intelligence community and, essentially, talk about what each of the elements of the intelligence community could do, how you could target Americans under that program if they didn't fall under 215 and 702, and a variety of other aspects of how the intelligence community operates. And so we have begun working on that last July [2014]. It's a challenging effort to look at how this massive authority applies, but we've been digging in and getting briefings from the intelligence community.

[There are] three aspects of Executive Order 12333 [that raise constitutional issues]. The first is separation of powers. 12333 is really based primarily on presidential power from Article II, the commander-in-chief power. The question is: To what extent, if Congress wanted to, could Congress legislate in this space in which the current president currently operates purely based on presidential power? Just a few months ago, Congress did legislate in this space with the Intelligence Reauthorization Act.[12] Section 309 [effectively] said that, under 12333, the government couldn't keep most records more than five years in its collection activities. So Congress, without a lot of debate on the constitutional side, went ahead and legislated in the space. [As part of our inquiry,] we're going to hear some discussion from academics on both sides of whether these are pure presidential powers or whether these are areas where the Congress can legislate.

We're also going to look at the First and Fourth Amendment and see where the President is operating on pure presidential power how much, if at all, do the First and Fourth Amendments restrict the President's power to conduct surveillance activities.

We'll also look at some of the operational aspects of 12333 including what oversight mechanisms are in place, because there is no judicial oversight of 12333 activities. Unlike 215, where a court now, after some reforms, has to approve every search of records and make sure the government has a reasonable articulable suspicion before the government does the search. And unlike 702, as I mentioned, at least a court approves the program, 12333 has no judicial oversight. And the question is: What types of oversight exist under 12333 that might compensate for the absence of judicial oversight? Congress has, of course, conducted oversight and is continuing to conduct oversight of these programs as well, but we're looking at, how effective that [12333] oversight function is.

So in conclusion, I think it's time now, with both the advances of technology and the government's abilities to collect information, that there be some reconsideration of the expectation of privacy standard, of the third party doctrine, and some better fleshing out of the foreign intelligence exception.

Thank you very much.

---

11. Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *reprinted as amended in* 50 U.S.C. 401 (2006).

12. Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293.