6-22-2015

The State of Surveillance Law (with transcript)

Jeffrey L. Vagle
University of Pennsylvania Carey Law School, jvagle@gsu.edu

Marcy Wheeler

University of Pennsylvania Law School
Case in Point: *The state of surveillance law*

June 23, 2015
Jeffrey Vagle and Marcy Wheeler examine the intricacies of U.S. surveillance law and the implications for civil liberties and national security.

EXPERTS

Jeffrey Vagle
Executive Director, Center for Technology, Innovation & Competition,
University of Pennsylvania Law School

Marcy Wheeler
Independent journalist, blogger, emptywheel.net

HOST

Steven Barnes
Host, Editor-in-Chief, Case in Point

Steven Barnes: Welcome to Case in Point, produced by the University of Pennsylvania Law School. I am your host, Steve Barnes. In this episode, we will be looking at the current state of U.S. surveillance law. We will examine what the future holds with the recent passage of the USA Freedom Act, and whether and how balance can be struck in America between national security, transparency, and civil liberties.

Joining us today to discuss these issues, first, we have Jeffrey Vagle, he is a lecturer here at Penn Law, and the Executive Director of Penn Law's Center for Technology, Innovation, and Competition.

Also, joining us from Michigan is Marcy Wheeler; an independent journalist who writes on national security and civil liberties. She blogs in depth on these issues on her site empty-wheel-dot-net.

So, let's begin. Jeff, we will start with you. What are the bases for U.S. surveillance law today?

Jeffrey Vagle: Well, it's a hodgepodge of laws that regulates surveillance all the way from municipalities all the way up to national security. But, when people think about surveillance today, they are probably thinking about one of three legal regimes. The first is – in no particular order, the first is the Patriot Act; the most famous section of this is Section 215, which was in the news recently. It's a very large act. Section 215 is just one small part of that.

We also have the Foreign Intelligence Surveillance Act as amended in 2008. The Foreign Intelligence Surveillance Act came out of recommendations from the Church Committee, in the seventies, which was in response to surveillance abuses in the sixties and seventies. And, it has since been amended many times. The most recent amendments of 2008 are what we are currently looking at. Section 702 of that act is probably what people are thinking of, again, in terms of national security surveillance.

And, then, lurking in the background is Executive Order 12333; this is a 1981 Executive Order from the Reagan Administration, and it is – not many people know exactly the scope of this Executive Order. Article II powers in the Constitution grant the president the power to enforce the laws and make the executive branch work, in effect. And, so, executive orders fall under that. This is – they do have force of law. They also can be challenged in courts, although Executive Order 12333 has not been seriously challenged in courts yet. That's trying to challenge national surveillance law is tricky in court.

The interpretation of Executive Order 12333 is of some concern. It's a very broad executive order having to do with intelligence gathering for national security purposes. But, as we have seen with Section 215, we have secret interpretations in effect of these laws. And, so, Executive Order 12333 is probably the broadest of those three legal regimes that I just discussed with respect to how much power does it grant U.S. agencies to conduct surveillance within the United States.

Steven Barnes: Marcy, do you want to add anything to that?

Marcy Wheeler: Just to give an idea of scope, the Section 215, which is what authorizes the phone dragnet, and as Jeff said, it's been much in the news. About a year ago, Richard Clark, who was just coming off serving on the president's review group for NSA activities, he said that 215 is a mere fraction of the data that gets collected. And the rest is EO 12333. So, when we talk about these authorities, what we know is the giant program that is the phone dragnet program collecting the phone records of every American is actually just a tiny bit compared to the EO 12333, which Jeff just walked you through.

Steven Barnes: Right. Do you have any inkling of what 12333 encompasses? Like what kind of practices or intelligence is collected?

Jeffrey Vagle: Well, herein lies the problem, right? We have – national security does require some amount of secrecy with respect to how certain agencies do their job. That's understandable. The problem that arises, and this falls under, this balancing act that we have to maintain between civil liberties and national security and safety, is that the government, whenever the government secretly interprets law, we don't have the natural adversarial process that our lawmaking usually has.

For example, the FISA Court, the court system that was set up as part of the Foreign Intelligence Surveillance Act, is a secret court. It's not an adversarial court. It is an Article III court. It does have Article III judges that sit on this court, but it's not adversarial. And by that I mean there is no second party. There is only one party, and that is the government, making an argument to a judge in secret with no one representing the other side to act as a force against the government. And, that's if anybody familiar with the U.S. Court System, it's a system based entirely on this adversarial system. Unlike other nations, civil law nations, which where the judge is actually driving the investigation, here we don't have that. The judge is a third party that's just watching this argument going back and forth between two parties, and that's worked pretty well. It breaks down when you remove one of those parties, and you only have one party making that argument.

Marcy Wheeler: One easy way to think about it is EO 12333 authorizes everything that happens overseas. We know that it does authorize some things inside the United States. That's

what Bush did, his Stellar Wind program, which has entirely moved to FISA, but it was this dragnet surveillance program up until 2004, 2007 range. But, what is interesting about it is that PCLOB, which is the Privacy and Civil Liberties Oversight Board, is looking into a couple of the 12333 programs to consider their privacy implications for Americans. And it has two in mind. We don't know what those two are. But, one of them, apparently, may involve collection within the United States. So, everything outside of the country with very narrow exceptions would be 12333. And we know, for example, NSA does a lot of bulk collection. It would also include covert activities. So, thinks like hacking, Stuxnet, would have been done under 12333 probably.

But, there are, as Jeff said, one of the tricks is that even with that easy breakdown, overseas 12333, domestic is FISA, there are still little cracks where 12333 authorizes stuff in the United States.

Steven Barnes: Thank you, Macy. That was great. So, for the purposes of our discussion here, it seems like for many Americans the concern is with the bulk collection programs targeting American citizens doing nothing illegal, just their emails or phone calls or Skype sessions get swept up in the NSA's program.

So, the USA Freedom Act passed June 2. How does it update existing law? And, what, in your analyses, are the strengths and weaknesses of USA Freedom?

Jeffrey Vagle: To address the first implied question that you had. One of – why Americans find this mass dragnet surveillance anathema is because it really does go against some of the founding principles behind the reasoning behind the Fourth Amendment. The Fourth Amendment of the Constitution does, it protects a person's, homes, papers, and effects from unreasonable search and seizure. There is a large body of law on the Fourth Amendment. And, one of the founding principles behind the Fourth Amendment was this idea that the founders found general warrants – warrants that were essentially fishing expeditions by the British Government at the time to be just completely unacceptable in their society.

So, what the Fourth Amendment does is it requires a particularized suspicion that is based on probable cause, sworn before a judge, that sort of thing. It does require a number of steps to obtain that warrant. And only then can the government come in and search the person, home, papers, and effects.

What these mass surveillance programs really are, are general warrant like programs. They are gathering data, metadata, and, again, for those that say well, it's just metadata, there is a whole line of arguments about why metadata is important. But it's this mass dragnet that is really just a fishing expedition. The intelligence community has said look, in order for us to find the needle, we need the entire haystack. That metaphor, Bruce Schneier has recently criticized that metaphor. But metaphors aside, we have to ask ourselves, under our system of laws, do we allow that sort of haystack gathering by government agencies of U.S. citizens?

Now, the USA Freedom Act was something of a response to this issue. It's the – Marcy, correct me if I am wrong, I believe it's the second version of the act; there as a first one that came out in – well, the second big – major version. The first one is, I think 2013 it was originally drafted. This one – the version that just passed is in some eyes weaker than the first one. But it does have a couple of provisions that are very important, one of which is this notion of having an amicus, a friend of the court present in the FISA Court proceedings. Meaning that it will be something closer to – I'm not sure it will be an actual adversarial process, but there will be someone there representing the people, in effect, to push back against some of these government arguments.

Marcy, I would be interested – what do you think about the efficacy of this amicus provision as part of the FISA Court in the Freedom Act?

Marcy Wheeler: It's a great first step and a necessary first step. But, one of the problems with it is that the executive branch is still allowed to claim any kind of privileges. So, for example, when Yahoo challenged, in 2007, the Protect America Act, which was the predecessor to FISA Amendments Act, when they challenged it, they worked with Mark Zwillinger, who was cleared – top secret clearance, yet most of the documents in question about what they were doing and what the government was asking Yahoo to do, and, importantly, where that data would go once it

came into the federal government and how it might be used against Americans. That was all privileged ORCON, originator controlled, which meant that the NSA, or whoever else originated the document, could say, well, I don't Yahoo to be able to see that, which they weren't able to. And, so, Yahoo was ultimately arguing in the dark, and there is very little to prevent that from happening going forward because the government can still claim, ORCON can still claim executive privilege.

The FISA Court now gets to decide whether any information is relevant but is not required to turn over all relevant information. And, so, this is what we have seen in the past, specifically with the Yahoo case, but not just with the Yahoo case, where the advocate is still arguing in the dark. But I sort of – l liken it to PCLOB, which I mentioned earlier, the Privacy and Civil Liberties Oversight Board, which was first instituted in 2004 as really an executive branch driven entity. And, then by 2006, 2007, Lanny Davis, who was the Democratic appointee on it, quit. He said, "I can't do my job because I am not being given information I need to." And, ultimately, in 2013, PCLOB finally became functional. And I think that's what this amicus position is going to do is it's going to start a process, and nine years down the road, we might see something that does what we need to do. But, I don't think it's all the way there yet precisely because the executive branch gets to decide how much information they want to share.

The same thing is true – one of the other provisions is that any significant FISA Court decision is supposed to be declassified. But, the Attorney General and Director of National Intelligence can say it's too sensitive. In that case they come up with a summary of what the decision was, but we have a sense from FOIAs for these same decisions what those summaries are going to look like, and they are not all that helpful to explain what the underlying law is.

So, again, these are important first steps. There is nothing wrong with them. But, we need to be realistic about the fact that the executive branch is really still able to decide whether they want to participate in this or not.

Jeffrey Vagle: There's another feature that I think was on the wish list for some that wanted a stronger USA Freedom Act, and that was strengthening the minimization procedures that

currently exist under FISA. So, minimization procedures are required by law so that if a government agency, while collecting data, inadvertently collects data that they shouldn't have – meaning it was in violation of the Fourth Amendment, or is any number of reasons. But, if they shouldn't have that data, and it was only inadvertent that they collected this data, they need to minimize these mistakes by getting rid of that data, culling the bad data out and only keeping the truly relevant data.

There are some rather large loopholes in the current minimization procedures, one of which is the fact that any information that is encrypted is automatically kept and stored by the NSA and other government agencies. And that means that – and that's regardless of where the information came from. So, if you and I have an encrypted conversation online, those data could be kept and not minimized under the current law, the current interpretation of the law.

It's problematic. I guess most people would say, well, I don't encrypt. When was the last time I encrypted anything? Well, if you're using a web page with your bank, for example, the little lock icon that shows up on your browser means that the packets that are being sent back and forth between you and your bank are encrypted for good reason. There's a reason why we don't want these data just out there in the clear. We have seen what happens when data are out in the clear.

So, that means that as our communications become encrypted more and more, even our – the sort of tacit communications, or communications where we are not explicitly encrypting, those data could potentially be kept and held for an indefinite period of time under the minimization procedures, which, I think, that's problematic. It is basically a large loophole around some of the reasoning behind these minimization procedures.

Steven Barnes: Marcy, anything to add to that?

Marcy Wheeler: Let me take a step back and explain the rest of the USA Freedom Act, just so that it is out there is that the key provision to it was an effort to limit what was called "bulk data". And to understand the bill, the law, now, you need to understand how the intelligence

community defines bulk, which is all. So, anything without a discriminator – so, when they collect all of the phone records in the United States, they do that by going to Verizon and saying "all". Going to AT&T and saying "all". And, so, what USA Freedom Act tried to do, both for Section 215, for pen register, FISA pen registers, and for NSLs, was to say we are going to make it so you can't collect bulk data anymore. But the way they did that wasn't – the first version of USA Freedom Act tried to say everything's got to be really directly relevant. You can't get information on somebody who doesn't have any tie to your suspect.

In this case, it still allows bulk e-collection because what it says is you need to use a specific selection term; therefore, a discriminator, to choose the data you are getting. So, you can still get, for example, pressure cookers purchased using VISA, which is an application that they could very well – it's been speculated, we know they have gotten pressure cooker and other precursor information using Section 215, and so they wouldn't be getting all VISA records, they would just be getting pressure cooker purchase records. But, you can see that that would be still tens of thousands of Americans who have no interest in making a bomb out of their pressure cooker.

Another example is if you use a stingray and target, say, my phone number, you are going to collect thousands, and maybe hundreds of thousands of other Americans along with the data that you are using to collect me. And NSA may well keep that to find out who else is in my vicinity.

The basic function of USA Freedom Act is to impose some upper limit on the kinds of collections that NSA and FBI – because much of this is done by FBI – can do. But, it's not as strong as a means to do so, and we should expect the NSA and FBI to continue to get these bulk e-collections. So, that's another basic thing about USA Freedom Act.

One really important detail about it, though, is, I talked earlier about EO 12333 and FISA authorized. There used to be an internet dragnet until 2011. It had legal problems because it's very hard to collect internet metadata without also collecting stuff that counts as content to telecoms. And, so, it was shut down from 2009 to 2010, and then came back online. And, then, in 2011, NSA was sort of like we're not going to do it this way anymore. And there is reason to believe a significant chunk of that is now done overseas. And that is possible because the way

the internet works, a lot of signals get routed overseas. That's all available to the NSA. They can collect it there with almost none of the restrictions that the FISA Court imposed, so they can use it for not just counterterrorism purposes, they can use it for counter-narcotics, they can use it for just foreign intelligence purposes. And, so, that collection is not affected by USA Freedom Act.

But, what probably happens under USA Freedom Act is that if you think about it, nobody uses old-style phones anymore, right? And there have been multiple reports of gaps in the NSA's collection because the metadata is limited to telephony data. There has been some indication they are not getting all cell phone data. That may have to do with 3G, 4G technology. They are probably not getting Skype data under that collection, which, if they are not getting, the entire dragnet would have been useless to prevent the Boston Marathon attack because one of the brothers had no working phone leading up to the attack. And, so, there is very good reason the believe, under USA Freedom Act, those additional kinds of phone data, which are not strictly speaking telephony data, will be collected in the much more limited call detail record program where NSA has to go to the providers to get specific two hops of communication. That's actually a significant change that should make the dragnet more effective, but also means more innocent people will get sucked in.

Steven Barnes: Let's just take a step back a little bit. So, based on the information that is currently available to the public, how effective has the Patriot Act been in addressing terrorism issues?

Jeffrey Vagle: Part of the problem is the definition of effective. There have been arguments by members of the intelligence community as well as their friends in Congress who have said that, for example, Section 215 is crucial, or essential. And, there have, in the past, been claims that Section 215 actually prevented attacks. Directly prevented attacks. That has been shown to be false. We have no direct evidence. As a matter of fact, a presidential commission, almost two years ago now, that took a look at the effectiveness of the anti-terror, or counterterrorism programs, including these intelligence programs, found that we don't have any evidence that these programs directly prevented a terrorist attack.

Now, there are some indirect successes. For example, after the Boston Marathon terror attacks, Section 215, or bulk metadata collection, was used, among other things, was used to verify that this was not part, or verify to the FBI's satisfaction that this was not part of a larger attack that was going on.

Similarly, the attacks, I believe in 2013 on overseas' U.S. Embassies, they used the same methods to verify that this was not part of a larger attack that was going to move to the United States. That could be attributed to 215 as an indirect benefit.

So, that is difficult to prove. It's the question of the benefits start from absolutely essential at the very top where we could not do our jobs without this. And that claim has been made. All the way down to well, it's a nice to have. The problem that we are having is that every one of these programs so far have been claimed by the intelligence community as being absolutely essential. That we could not do our job without this.

What we have seen is that some of them have been outright falsehoods or the least untruthful answers. That has made Americans skeptical of these claims. It's a bit of crying wolf on the part of the intelligence community, and especially when we have presidential committees formed to look at the question whether or not these are actually effective, and they come back with a somewhat negative answer. It makes the population even more skeptical, especially when we are talking about this balancing act. If, for sake of argument, if we are to give up civil liberties in exchange for security, well, if these programs that we have given up our civil liberties for aren't actually providing any security, at least not in any direct, demonstrable way, then, we start to wonder well, this is kind of a bad bargain.

So, when – now that the dust is settling on this Section 215 argument, it's there was some people had the impression that Section 215 was about to be repealed. There were many of us, Marcy included, had to tell people, no, calm down, Section 215 is huge. It was really just about the sun setting of three provisions, two of which I don't think have ever been used.

Marcy Wheeler: One hasn't been used. The roving wiretap, so, what hasn't been used is Lone Wolf—

Jeffrey Vagle: Lone Wolf, yes.

Marcy Wheeler: -- although that's the kind of thing that FBI might redefine in secret, and there is reason to believe they did that. Roving wiretap, which if I keep changing phones, it says I am going to wiretap Marcy Wheeler, and I can tap any new phone she adopts. That's how it's used, and it is actually used, I have seen, a couple hundred times a year, but that is not an official, from reports. But that was also used as a secret reinterpretation by the FISA Court in 2007 rather than to target one person, Marcy Wheeler, for example, it targeted all of Al-Qaeda, and, so, that allowed the NSA to just wiretap whatever new account they believed was part of Al-Qaeda, which is an expansion, and probably a not faithful interpretation of what the law says. Again, that's the problem with the FISA Court.

But I think it's Section 215 generally, and this is a point Jeff just made, but it's really worth reminding people is the phone dragnet is just one part of Section 215. A recent DoJ, DoJ IG report said that in its use through 2009, no FBI agent had been able to say it had broken a case. And that's all uses. That's the phone dragnet, which maybe about two percent was useful either for finding a terrorist or finding somebody who could become an informant or finding somebody who could be deported, which is how the FBI measured it. So, two percent usefulness of the phone dragnet through, basically, 2006.

But, then, there are these other uses. I talked about collecting purchase records for explosive precursors, other kinds of business records. What's interesting about this is Section 215 can be used both for counterterrorism and for espionage, which is broadly interpreted to include cyber security. In 2009, the FBI kind of shifted and started doing a bunch of internet collection using Section 215. So, what I just told you about the DoJ IG's finding through 2009, it may have changed. And given the kind of responses from FBI, I suspect it has changed, but I suspect that this use to get internet data, which they say they use for both cyber security and for terrorism

purposes, I bet that's useful. They say they have no other way of getting that data, so, that's probably useful, but they won't tell us how.

Other than that, I think the phone dragnet is useful primarily for finding informants, which they don't really want to talk about, but they use this very valuable metadata to find who is in the right place to inform on other people. Also, we know that they use this metadata, both via the 215 and the 12333 metadata to establish particularity for FISA Amendment Act, and this is something that came out of the Yahoo challenge. So, in other words, they get by legal questions about other collection by saying we've selected this person – we've proven this person is of interest to counterterrorism purposes or to some other kind of purposes by using this metadata to show their value.

That's that the intelligence community is really talking about when they talk about its value, but they don't really want to explain all of that to you because it would, you know, sources and methods.

Steven Barnes: That makes perfect sense, so, I would assume the intelligence community would argue, as you have both explained that these programs are used to target people, groups like Al-Qaeda, to target people who may be involved in terrorism operations, or, perhaps support. Not so much concerned with how much I binge watch "Veep" on my tablet, for example. So, how—

Marcy Wheeler: It's true of the telephone program. But, again, what they are collecting overseas under 12333 is much broader, and they are collecting viewing – I mean, they are probably doing some of that with the 215 internet collection as well. But, they are doing what kind of search you are doing, what your internet cookies do. We know that they have collected porn watching habits, including off of U.S. persons. So, they do collect that. But most of that falls under stuff collected overseas, although some of it probably comes from 702 as well. And the way in which they use all of these together does get to that kind of question. They may not look at you unless via the phone dragnet program they have discovered you are two degrees away from somebody of suspicion.

But, remember that's a ton of people. Like if it were just the direct contacts of suspected terrorists, it would be one thing, but they are doing it another hop out, so that's at least an order of magnitude more, right? Any of those people can be subject to – and it's in the phone dragnet orders the phrase they use is the full analytical – I forget the – I love the term, but they basically say once you hit that two degrees of separation, they you can be subjected to anything that the NSA has, which means then they may start looking into your prom watching habits of what kind of searches you do online. And that's when I think you start to see the privacy implications for completely innocent people who are just two degrees away from somebody of interest.

Steven Barnes: Right, so, is it even possible, but how do we strike the proper balance between national security, civil liberties, and transparency so the public can be informed to a degree that satisfies both the public as well as the national security and intelligence communities?

Jeffrey Vagle: As Marcy pointed out, the USA Freedom Act is a good first step. I don't think it's the end of this battle in any way. One thing, we have been talking about this sort of in the background, when the intelligence community is making their arguments before Congress or before the American people, what we have found is their use of terms that we have been using today in a colloquial sense, collect, for example, they don't mean the same thing that we do when we say collect. So, when they're saying "we're not collecting everybody's data", they mean that they are not doing searches on these giant databases that have been built by collection in our sense of the term. So, they are relying on a bit of a semantic difference, a somewhat artificial semantic difference I think some people would argue, about the meanings of these terms. That goes to a larger question that we saw, not just in the last five or ten years but also going back to the seventies and the Church Committee. Many of these issues may be able to be solved if the intelligence community was a bit more forthcoming about what they are trying to accomplish, what their goals are with these programs, and, truly, how effective they are.

Part of the problem has been that every time one of these programs has been questioned, the first response, almost always, apart from silence, but once you get past the silenced, the intelligence community comes out saying "these are absolutely essential". Well, if the programs are truly,

absolutely essential, there needs to be a better case, and this better case made before the American people. We don't need to see all the secrets necessarily, we understand that some of the secrecy is necessary. But there has to be a better transparency balance because when you do have this curtain that is set up and you don't know what's going on behind the curtain, you are setting a system that is very vulnerable to abuse, as we saw in the fifties, sixties, and seventies, and as we are seeing again today. It's interesting, actually, I think a very meaningful point that the Second Circuit when, in their decision on ACLU v. Clapper, actually brought up the Church Committee and said look, we are heading to the exact same kind of situation that the Church Committee was dealing with.

Now, those laws, FISA is still on the books. It's amended – been amended since then, but the principles are still the same. And we look at what the intelligence community is saying, we look at what the law says in striking this balance, and we say why do we keep on reinventing this wheel? And, as Justice Sandra Day O'Connor said in a decision that the time to consider whether or not to adjust the balance with our constitutional civil liberties and the values behind them with national security is not during time of crisis. We have seen over and over that when we do make, frankly, rash decisions in times of crisis, we end up with things like the Espionage Act and the abuses that took place during World War I around that. We have the internments of Japanese Americans. And that we have Guantanamo. And we have these, now again, these intelligence abuses.

So, transparency is key. And the balance – we have always, as a nation, said that if you are going to tip the balance in any direction, it must be tipped towards civil liberties. And that is the bargain that we make. We are never going to have perfect security; that is just an impossibility. So, do we chase our tail trying to achieve that perfect security? Or, do we realize that no, living in a country where we have strong civil liberties is more important than trying to chase this ethereal goal of perfect security. That's where that – the conversation there is no right answer to that question, of course, but it helps if we have an honest discussion and we get some of these ideas out in the sunlight for examination and so we can make truly informed decisions.

Marcy Wheeler: I would add – I think there are three ways that we can radically improve transparency. One is we need to improve the technical skills available to congressional overseers. You do that partly by expanding the intelligence communities and making sure there are more technical people on it. But, also, by ensuring that more members of Congress can review things. Congressmen Lieu and Hurd right now are kind of leading the charge against preventing encryption. They are both computer science graduates, and, so, bipartisan, really aggressive opposition to the FBI's, in turn, opposition to encryption. But, they are very rare members of Congress, who know what they are talking about when they are talking about encryption. So, I would say the very limited control over these secrets by the intelligence committees is not working, and it needs to be broadened, especially in the House.

Another area that really, really needs to be fixed is that the FBI is not asked to come up with the metrics to measure the impact of this. So, the FBI doesn't have to count how many backdoor searches, how many searches – warrantless searches of content they get off of Americans' names. And there's a bunch of other things they don't collect either. So, when Congress says we are sure there is no privacy problem, when Congress says under CISA, which is, of course, being debated today, we are sure there is not going to be any privacy problems; it is impossible for them to make those claims because right now FBI simply isn't collecting the data and providing the data to Congress to be able to do that.

Another example is in USA Freedom Act, an improvement over the past version is for the first time, the government has to tell Congress how they are using PRTT and which agencies. That's new, but it suggests that other agencies, like DEA, have been using it and not reporting to Congress.

Steven Barnes: PRTT is what?

Marcy Wheeler: Pen Register – probably location data collection. But, they have, again, all of a sudden, after years of this collection going on, this bill says you got to tell us what it does. Another report that they are requiring anew is basically bulk collection, bulk e-collection under Section 215 has to be reported and the kinds of minimization. That didn't go to Congress before.

So, these metrics need to be in place for Congress to be able to do their job and the FBI, in particular, is very hesitant to develop the metrics. And, in a related issue is the FBI is hiding all this from defendants. So, for years the government said well, no one's – that 35 judges have found the phone dragnet constitutional, only one defendant has even been able to begin to challenge the use of Section 215, and he is the only one they have actually caught. But, every other defendant hasn't gotten notice on it.

Defendants aren't getting notice on this pen register stuff, which is probably location data. Defendants aren't getting notice on EO 12333 collection. And, unless defendants get notice, the people who have the standing to challenge this so that we can have that adversarial process of testing whether this stuff is constitutional unless they get notice then you really aren't testing, you really can't say that the stuff is illegal because it's mostly for the – largely hidden from judges, still.

Steven Barnes: That ties into my next question. For you, Marcy, what kinds of surveillance laws are in place now that aren't getting the attention, or the scrutiny, perhaps, that they should, in your view?

Marcy Wheeler: To my mind, I'm grateful for Edward Snowden, but the focus on NSA has been misplaced because since 2008, the government has made a very conscientious effort to move FBI to the forefront of this process. So that, for example, big chunks of 215 data get delivered in raw form to the FBI. And the FBI can access that data both as it comes in, but it rests in their databases for 30 years. The FBI can access that data not just if they are conducting an investigation into somebody for terrorism, but at the assessment level. So, whether they have a tip without any real evidence of wrongdoing, whether they are looking for informants, whether they are trying to find what the map of the Somali community in the Twin Cities looks like. For all of those purposes, they can go in and access this content, and then kind of send it on into a black box with the FBI, and you will never know. Defendants will never know that that's what elicited their criminal investigation.

That's true of 702 content, it's true of traditional FISA content, it's true of pen register. All of these techniques have become, have been dumped into this black box at FBI, and they are affecting people's lives and people aren't really being given the opportunity to challenge it, or to even know about it.

As I said, one of the most interesting cases in recent years is a guy named Reaz Qadir Khan, who was charged for, in conjunction with an associate committing a suicide terrorist attack in Pakistan in 2009. And because of the timing of it, he clearly was, he would have – these illegal, or questionable illegal surveillance authorities would have been used against him. His lawyer challenged them and said we want a list of everything, and the government fought back. But, the judge in that case was Michael Moseman, who is a FISA judge. For almost the first time, he's like we will deal with this in CIPA. We will deal with it as part of the secret process of what the government has to tell me because he knew what's there. He's one of the 11 judges who knows what's really going on. And, then, within weeks after he made that decision, the government settled.

So, it's a really interesting case where if the judges knew what they were looking at, they might demand a lot more accountability from the government, and the government might not press some of the same criminal cases that really are based in illegal, or questionably legal methods.

Steven Barnes: And CIPA is?

Marcy Wheeler: Gosh, what does it – Classified Information Protection Act, which is just the means by which the government can use classified information in criminal trials and substitute information such that the defendant can still challenge it or use it, but the classified information won't be disclosed either to the defendant or in court.

Steven Barnes: Any reaction to that, Jeff?

Jeffrey Vagle: I think the issue of transparency is the elephant in the room, here. I think that when we are talking about the effectiveness, or non-effectiveness of any of these laws, and how

they are actually being applied, really does benefit from a little bit of sunshine, as we saw in the case that Marcy just mentioned. And there are a couple of others that when pushed, the government has chosen to settle. Two things that are happening here.

One, it's an interesting fact; however, you feel about the guy, we would not, probably not be having this conversation were it not for the revelations of Ed Snowden. That's unfortunate for a lot of reasons but mainly is some of these things are clearly relevant to us, as American citizens, and to others. And the fact that the only way that it could ever get out was through, arguably, illegal means, is troubling.

The other part is that when we talk about surveillance, I think we tend to think of, especially in the post-Snowden era, we tend to think of NSA, FBI, CIA, the basically tech surveillance we're talking about. It's email, cell phone, that sort of thing. When surveillance is really a much bigger issue. It goes, it's all the way to – from super high-tech surveillance to no tech surveillance. And that's the police just patrolling, for example. Surveillance by itself is, it's a value-free term. It's not a good or a bad thing, it's just a thing, and versions of surveillance are necessary, as we found, for a working society. The question is, well, how much of that are we willing to deal with? As we become more used to these programs, the fact that you, yourself, or I have nothing to hide – this is the "nothing to hide" argument that you hear all time – is not relevant because I cannot speak for everyone in this country. What nothing to hide means depends on what they are looking for. They, being whoever is doing the surveilling.

So, as we saw in the abuses of the fifties, sixties, and seventies, Martin Luther King probably had, in our eyes, nothing to hide. He had an extramarital affair; he was illegally recorded during that. The FBI, infamously, and anonymously, sent him a note that said "you should really kill yourself, Dr. King" because we have this information. These are clearly abuses. If we, little but little, like the proverbial boiling frog, if we start to allow these abuses and hide them, and say well, I, personally have nothing to lose here. We, as a society, start to lose out because we are seeing and have seen, for many years, this encroaching effect of a greater surveillance society growing in the U.S, and other countries.

Prime Minister Cameron famously said recently that for too long British citizens have gone along with not being surveilled with the assumption that just because they are law-abiding citizens. The implication there is like, well, a law-abiding citizen is no longer a barrier to surveillance. It's a dangerous road to go down. And this halo effect, the reason why we – there are many of us in the community that push back and question these program sis because we don't want to, necessarily, go down that road. We have a strong constitutional incentive to avoid these sorts of regimes, and this is why we question these things, and this is why transparency is so vital to this process.

Steven Barnes: Let's take this down to sort of an everyday level. In terms of thinking about these issues, what should the average person, with a Smartphone or tablet or just connected to the internet, be thinking about in terms of how the technologies they use every day intersect with these legal issues?

Marcy Wheeler: For the average person, they are more likely to be targeted by criminals than they are by NSA. But, even there, some of the same methods are useful. So, in other words, strong passwords. Use encryption while you can. One of the problems with the FBI's campaign against encrypting phones is that there is something like one-point-one-I don't know the exact number, but there are a huge number of Smartphones stolen every year. And if your phone is encrypted, then people who are trying to use the phone to steal your data, to steal your identity, aren't going to be able to use it.

The same also happens to be true if the NSA is trying to spy on you because you are a Muslim cleric. But, I think there is a notion of hygiene that applies to both whether you are going to lose your identity because you shopped at TJ Maxx, or whether the NSA is going to come after you.

I also think that just as a comparison, there was this report of a really devastating hack of the Office of Personnel Management last week, which it somewhere between two and four million government workers, and got very, very personal data off of those government workers, and it is going to expose them to spying going forward. That's the same kind of bulk data that the NSA collects overseas. And the NSA does not limit itself to government employees. We know that

they go after tech employees. We know they go after tech company executives and search for proliferators. And, so, that's the mindset. If OPM's hack is bad, and it is, then we, as a society need to really consider what is a legitimate target for government hacking – what kind of data should be kept, whether it is a target or the government. Because that data is going to be vulnerable out there, and you can be compromised in any number of ways.

Steven Barnes: Anything to add to that, Jeff?

Jeffrey Vagle: Another example of this issue is the FBI's – and Marcy alluded to it – the FBI's recent call for encryption back doors or security back doors. It was, the conversation was started last winter when Apple and Google both announced that they were going to encrypt their customers' communication – certain customers' communications in such a way that not even Apple or Google could get at it. It was between the sender and the receiver, and that encryption could not be – there was no was that they could reverse that process.

The FBI Director, Comey, and others came out against that policy and said, no, we should not have a no-go zone where not even – where law enforcement couldn't go, even if we had a legal right to go.

The problem with that – a problem with that argument is that from a purely technical point of view, we don't know of any good way to do what – to create this back door, or front door, or whatever it is you want to call it – we don't have a way of doing that. Back in the early nineties, mid- nineties, we had what we laughingly referred to as the first crypto wars where the government was talking about creating a key escrow system where whenever you wanted to use strong encryption, you would create two keys. One – well, it's a little more complicated than that, but basically the government would have a master key that they would put in escrow. And then, if they had to, if they got a warrant, and that sort of thing, they would be able to unlock the encryption. It doesn't work.

A professor here at University of Pennsylvania, Matt Blaze famously discovered a flaw in this encryption scheme – or decryption scheme, as it was, and, now, we are having that same

conversation again. And it's just – it's complicated. It's beyond the scope of this conversation, but many people in this field, the technical people, engineers, computer scientists, have gone before Congress and said that is a bad idea. Yet, we are still having the conversation. The FBI has not backed off from that request. And this is a very real concern because it's, with the FBI, the NSA, they have both a defensive and an offensive side of the house. So, for example, the NSA has an offensive side where they are doing hacking of targets that they are interested in getting that data. They break into systems and that sort of thing. But, they also have a defensive role, a defensive mission, which is defending the cybersecurity – there, I said cyber, but the cyber security defense is of their missions.

So, you have these conflicting missions. And if we do something, let's just say that there was some system set up where back doors were created, it is almost certainly going to weaken – well, not almost certainly, it will weaken our defenses, not just of power grids and that sort of thing that we are working on. But, the same thing that we are worried about that Marcy was talking about with respect to criminality – our personal financial data, our personal data can be grabbed. And, as we found, when you have a patient, well-funded adversary, what used to be referred to as an advanced persistent threat, and often times, they are affiliated with the governments, but not necessarily, they're not just after the quick smash and grab. They don't just want your credit card number. They are going to patiently gather all kinds of different kinds of data. So, that with the IRS breach that we saw recently, they could actually combine data to get past the IRS's rather weak security mechanism to file taxes on your behalf and get refunds back illegally.

So, many people were finding this past tax year that the IRS acknowledged, hey, we got your tax return. And they said, I haven't filed my taxes yet, and we're talking about tens of millions – actually, I think the number is over a hundred million dollars' worth of fraudulent tax refunds that were sent out using this rather ingenious, or somewhat ingenious, but a very patient scheme. And, again, to Marcy's point, we have to decide what legitimate targets are because that sort of scheme is exactly what the NSA is doing also on the offensive side of the house. So, these are important questions that we have to decide as a nation.

Steven Barnes: Related to that, Marcy, you are very well known for going through just troves and troves of data, these so-called document dumps by governments, and other agencies. So, first question, what kind of information are you seeing as part of that? And, how can the wider public be better informed, keeping in mind, most people don't do what you do in terms of getting at these data troves?

Marcy Wheeler: Most people have a better life than me, huh? You know what, the office of Director of National Intelligence, so, James Clapper's office, I think adopted a very deliberate strategy after the Snowden leaks to flood people with transparency. They have released a ton of information about all of the phone dragnet orders, for example, are available. And there are very subtle aspects about changes in that program, which are available. You know that Verizon changed their delivery in 2007. You know that there is a new emergency provision. You know that they probably abused that already. You can see trends in data. So, when the FBI started using Section 215 to get internet data, the numbers exploded – I mean, they are still relatively small, but it's like 200 orders, but those orders could be hundreds of thousands of people, and, so, those are when questions should be asked.

We also know that the FISA Court started imposing minimization procedures on those orders. And that's the kind of stuff that's out there. I don't actually think the privacy community has done a very good job of using that transparency and there's a lot of stuff – I even – I know this stuff pretty well, but there was a part of USA Freedom Act, which I should have realized, was going to authorize the use of data that probably was collected illegally. And I just forgot you know, I just. So, that data is out there. Maybe it will stop under a new president, maybe it won't.

But, what you have to do, I think, with that knowledge is then to be able to come up with an understanding of – and user impact. As I say, it always comes back to the FBI because they are the ones that can put you in jail. And that picture still isn't there yet, either.

For your average person, you shouldn't be working at that level of data. But, you should be asking the kinds of questions of your member of Congress, how does the NSA dragnet connect

to the people who can put me in jail? The FBI? I guarantee you, 300 members of Congress could not answer that. Probably more than that. And, if they cannot answer that then you should insist that they try and get that information because our advocate, our representative for being able to exercise some kind of democratic control over this are our members of Congress, and they just don't know enough about it. And, to some degree, they are not allowed to know enough about it. But, until they start asking those questions, then the NSA and the FBI and the CIA will continue to operate in the dark without much accountability because no one is asking the right questions.

Jeffrey Vagle: Marcy sells herself short here. No serious student of surveillance law, I think, does not follow Marcy at her blog. Not just fans, but detractors. She gets into some rather interesting fights with people across the spectrum. But, that said, there are a number of sites like hers, which are probably at a deeper level than most people would be interested in. But, one thing I have noticed is that over the past decade or so, newspapers like the *Washington Post* and the *New York Times* have actually done a very good job of expanding their national security desks and doing really, true investigative journalism into these issues.

And, as we saw with the *Guardian* and the *Washington Post* and the *New York Times*, to some extent, they have been rewarded with Pulitzers and other awards. So, I commend some – not all, but some of these newspapers for really taking this issue seriously and trying to get at what some of the core issues are – get past some of the technical weeds and the legality – or the legalism, and get to the true, core issues of what we, as citizens should be concerned about.

Steven Barnes: Marcy, you talked a little bit about elected officials. Jeff, you talked about some of the better coverage you have seen in the media, so whatever a position a person has, who is a U.S. citizen, on these issues, how can they make their voice heard? Is it through contacting their member of Congress? Is it through reading up more? Is it through participating in town halls? How do you make your voice heard to people?

Jeffrey Vagle: I think right now the conversation is at the national level, so we are really talking about member of Congress, your representative, or senator. And, unfortunately, mileage varies

with respect to the member of Congress. We have some members of Congress with technical degrees that really understand this and can put this in terms that everybody can understand, do that translation. And, then, we have others, who I won't name, but don't even use email. You know their staff is using email, but they famously say "I don't touch the stuff". That's problematic. We live in a highly technological society. I think members of Congress are not doing us any services by not at least attempting to understand these issues. And, but forcing, or at least pushing members of Congress in this area; however, you feel about it, oversight is important, and we have seen a kind of a hodgepodge approach to oversight. Much of it, in the early days, was relatively bad, almost no oversight. Now, we are seeing a little bit more of it. But, it really depends on members of Congress that understand these issues. They don't necessarily have to be computer scientists, like some of them are, but to make an effort and just say well, I don't do email. That's not acceptable anymore in today's day and age.

So, I think that pushing your member of Congress, questioning them, and getting those answers – the satisfactory answers; however, you come down on – wherever you are on the political spectrum, I think we deserve some of these answers.

Marcy Wheeler: I would add, though, don't give up on local involvement. There has been a real effort in the last couple years to bring transparency to stingray use, which is a kind of technology that allows the user, which may or may not just be the government, to pretend to be a cell phone tower and with it collect a lot of data about your phone and everyone else nearby you. And, both the national level, things like the ACLU trying to FOIA the ways in which local police departments are using them, but also at the local level where people are going in and saying we need to know exactly how the police are using it, how much they are using it. It's brought a lot of transparency to the issue. And one of the things that has come out of that is not just that some police departments are not getting any legal process for these stingrays, and some are, but also that the judges have not been told what they are approving. You really need to have this kind of level of transparency for the magistrate judges, who are the ones approving these, to really understand what these new technologies entail.

Steven Barnes: Well, Marcy, Jeff, this has been a really illuminating, eye-opening discussion with some really compelling recommendations and analyses. So, I want to thank you both for joining us today. Some great discussion, and I want to thank everyone for joining us here at Case in Point.

[01:03:40]