June 28, 2017

Annual Conference Transcript

Surveillance and Privacy: Can They Coexist?

Hon. Matthew Olsen
Former Director, NCTC

Liza Goitein, Co-Director, Liberty and National Security Program
Brennan Center for Justice

Carrie Cordero, Counsel
ZwillGen PLLC

Ben Wizner, Project Director
American Civil Liberties Union

Ellen Nakashima, National Security Reporter
The Washington Post

Adam Klein, Senior Fellow
Center for a New American Security

Begin Transcript

ADAM KLEIN: (In progress) – so since 9/11, our intelligence community has developed powerful, sophisticated surveillance capabilities for the digital age. Now, for years these developments stayed in the shadows, popping up occasionally in major newspapers but the significance of those reports wasn't really appreciated until 2013, when a certain set of disclosures triggered a massive global debate that continues today.

Now, our leader in CNAS, Michèle Flournoy, likes to say that our job is to go to the (pain ?). What she means by that is we have to take on the difficult issues that policymakers need answers on. In that spirit, CNAS has entered this debate and discussion over the future of surveillance policy. Last December, Michèle, Richard Fontaine and I issued a lengthy report with 61 recommendations to guide the future of surveillance policy. Since then, we've continued

to build out our capabilities in this area, adding former Director of National Intelligence Jim Clapper as a distinguished adjunct fellow and also Matt Olsen, whom I'll introduce momentarily.

So, with that, let me introduce our panel for this lunch discussion. We've brought you some of the most thoughtful, most interesting, insightful and knowledgeable people operating in this space around surveillance, privacy, civil liberties and technology.

So, first, Matt Olsen, whom I just mentioned. Matt is the former director of the National Counterterrorism Center. Before that, he was general counsel at NSA. He's currently at IronNet Cybersecurity, which, coincidentally, was founded by Keith Alexander, the legendary former head of NSA.

MATTHEW OLSEN: It's not really a coincidence, not totally a coincidence.

MR. KLEIN: There was a bit irony there, which I think everyone else detected. And he's also served in various impressive roles in the Department of Justice. And Matt is now an adjunct senior fellow with us at CNAS and a huge asset to us.

Carrie Cordero, just to my left, is counsel at ZwillGen PLLC, which is a boutique national security law firm here in Washington. She's also an adjunct professor at Georgetown law, where she teaches, of course, national security law. Carrie appears frequently in the media and television, radio, publishes widely, including on "Lawfare." She also served in the national security division at DOJ and in the Office of the Director of National Intelligence when some of the crucial surveillance powers that we have today and that are being debated currently were crafted.

Both Carrie and Matt – and this is a key point for our debate today – are among the very select group of lawyers who have practiced before the secret Foreign Intelligence Surveillance Court which decides on government surveillance applications.

Here in the middle, we have Liza Goitein. I'm going to correct my pronunciation now just to get it out of the way.

ELIZABETH GOITEIN: You did it so much better than the senators did on the committee yesterday.

MR. KLEIN: Okay. Good. That's good to hear. She's co-director of the Liberty and National Security Program at the Brennan Center for Justice. Before that, she worked as counsel to Senator Russ Feingold on the Senate Judiciary Committee's Constitution Subcommittee. Liza is also a frequent commentator in the press, on the television, on the radio, a prolific writer on surveillance, national security legal issues, and civil liberties.

The empty seat represents Ben Wizner. I'll give him a very short introduction since he's not here. He is Edward Snowden's lawyer. I'll just leave it at that. Hopefully, he'll turn up. His Amtrak has apparently been delayed – surprise, surprise.

And then, finally, my co-moderator for today is Ellen Nakashima. She is a national security reporter for the "Washington Post," who's a must-read on everything related to intelligence, cyber security. Last week, she and two colleagues published a blockbuster 8,000-word story on what the Obama administration knew about Russia's role in the election last year and how they responded to it. That story has been triggering responses at the highest levels of government, including a few tweets from a certain official at the very highest level of government. With that, I'll turn it over to Ellen.

ELLEN NAKASHIMA: Thank you. Thank you, Adam. And thank you everyone for being here. As Adam mentioned, we are going to do a panel here with some pretty high-level questions. We're going to dispense with the introductory remarks and make this more sort of conversational and free flowing. So I think I'll start with some propositions and big-level questions.

And the first one I will pitch to the group here is: can secret oversight be meaningful oversight? So you have the FISA Court, as Adam mentioned. You have the NSA's inspector generals. You have the Congressional Intelligence Committees. These all tend to do their work in private and rarely, if ever, publish public opinions or reports. So how can the public be confident that these oversight bodies are catching and correcting abuses or are not interpreting authorities in any way that's unjustified? Can secret oversight be meaningful oversight?

Liza, you want to start.

MS. GOITEIN: Sure. I would say that secret oversight is vastly preferable to no oversight, which is – or at least to very little oversight, which is what was happening essentially before the current intelligence oversight structure sprung up beginning in the last 1970s. But it has its limitations and in at least one sense, I think it can sometimes actually be counterproductive.

So the limitations are specific to the branches that do the oversight. The limitations of secret congressional oversight – and I'm talking about the work that the intelligence committees do, for example, which those committees do that work mostly in secret – those limitations are set forth I think very well in Jack Goldsmith's book, "Power and Constraint," which I would recommend to anyone who hasn't read it, in which he talks about the fact that members of these committees don't have the usual political incentives to do rigorous oversight. They can't sort of splash what they're doing all over constituent newsletters. They can't go to their donors and say, look what I did for you. And so they just don't have the same sort of political rewards for sticking their necks out and picking fights with the executive branch.

That doesn't make their oversight meaningless at all, but it limits their oversight. I would also say – and to the extent they're dealing in secret information that sometimes the executive branch will not share with the full committees, that's a problem as well. In the judicial branch, secret oversight often means no adversarial process. And when courts operate outside the adversarial process, it doesn't work very well, frankly. It's just not a very effective way for

courts to do their jobs. The adversarial process is not merely about fairness, it's about being the best way to get to the truth.

And then, executive internal oversight I think, there is a risk that there isn't going to be follow-up on that oversight when there isn't publicity. So when an inspector general reports are public, they can create a drumbeat for reforms. But when those reports are secret, you're much less likely to see the necessary follow-ups and so there's no requirement necessarily that agencies follow-up on inspector general recommendations. And I think that's one reason, for example, the Department of Justice Inspector General has been very effective is that those IGs have managed to declassify and make public many of their reports.

Just very quickly, the one way in which I think sometimes it can be counterproductive is that I think that the existence of these oversight mechanisms and the deployment of these mechanisms can sometimes give lawmakers the confidence or in some cases the cover to support executive – laws that allow what I would consider to be overreach because they will give substantive authorities that they might not otherwise feel comfortable giving, saying, it's okay, the inspectors general are going to look at it, so we don't have to worry.

MS. NAKASHIMA: Matt, or –

MR. OLSEN: Sure. I agree more or less with what Liza said. I mean, I do think it's worth going back to, as Liza said, you know, the difference between secret oversight and no oversight. If you go back to the 1970s, before the real reforms that were put in place following the Church Committee and all the abuses that were uncovered through the Church Committee, you know, you have a situation, really there was almost no oversight of executive branch intelligence activities.

In fact, there's this great moment in one of the hearings in the Church Committee where an NSA official, a top official is asked about the review that they undertook of the legality of those activities and his answer was, well, we really didn't think about that, which is kind of an astounding thing. And I'll tell you that it's very different, having served as NSA general counsel, very different to how the agency operates today where, you know, I and our lawyers were involved in every significant decision, policy, legal, operational decision that the agency was making.

And that's really a function in large part of the changes that were put in place in the 1970s where you had three branches of government involved in the oversight of surveillance activities in particular – the FISA court, the congressional intelligence committees, and then executive branch oversight through general counsel, the inspectors general.

So as I think about it, I do think that – I think this sort of follows on Liza's point, which is one – you know, the features of effective oversight even in secret have to be – one feature has to be the separation of powers, that you separate the oversight responsibilities among the three branches. That's something that was achieved with intelligence oversight now, as well as making sure that there's sufficient disclosures required in order to inform that oversight, and then

resources are given so, for example, you don't have committees with no people to actually do the oversight so there has to be resources behind it.

And if those features are put in place, then secret oversight can be effective. And the last point I would say is just that, you know, as much as secret oversight sounds like an oxymoron, it's a reality that we have – I believe we have to accept when it comes to oversight of espionage because you can't have it be totally public. It just would undermine the ability to carry out spying activities if it was done in public.

MS. NAKASHIMA: So there's also the issue, though, of – isn't there a sort of like agency capture on the committees? If you're an intelligence community and you are conducting this oversight all the time you're in with the intelligence agency, you're getting to understand really in depth what they're doing, why, how important it is, you start to see things from their point of view. And because often you can't reveal what they're doing to the public, is there a risk that you become captured in a sense by their mindset and are not willing to, you know, blow the whistle on something that might be slightly, you know, problematic?

What do you think, Carrie or Matt?

CARRIE CORDERO: Well, we're talking about a couple of different types of oversight, right?

MS. NAKASHIMA: Sure.

MS. CORDERO: So there's the executive branch piece, which is the internal executive branch oversight. And what are we talking about oversight of? We're talking about intelligence oversight of classified surveillance activities that are intended to conduct – to collect foreign intelligence information, so information about espionage, information about national security, information about foreign affairs. And so this is all information that is traditionally in the classified realm and so the question is is how do you do effective oversight of that type of activity that is – by necessity needs to be closely held?

On the congressional piece, I think what we've seen is that the membership and the leadership matters who the leadership is of the intelligence committees, so I think in all of our experience and in our government experience, we've seen chairs and co-chairs that work effectively together to conduct serious, robust oversight. And then there's other tenures on the committees that I think reasonable observers would look at and question whether or not they are committed – those individuals are committed to conducting effective oversight.

But I think what we're really sort of struggling with in this current environment is a real questioning of whether the deal that was struck in the late 1970s, which designated to the congressional intelligence committees that they were going to be the committees, the House Intelligence Committee and the Senate Intelligence Committee, that they were going to be the intelligence committees that were going to do oversight of these types of issues on behalf of the rest of Congress, which, of course, then is representative of the public.

And where I think we're seeing stressors eight now really goes to the very legitimacy of that process. Are there other members of Congress who want to be better informed about issues regarding surveillance and privacy and national security because they're going to have to vote on legislation, and are the members of Congress and is the public satisfied with delegating this authority purely to the intelligence committees or do the intelligence committees and the executive branch need to do a better job of informing more members of Congress regarding how the intelligence community is doing its work – not necessarily at the same level of detail, but more than perhaps what's been done in the past.

MS. GOITEIN: And I can I just do a quick follow-on to that, which is that under the National Security Act, the intelligence committees are not only supposed to be the proxies for the rest of Congress, they're supposed to be the gatekeepers and they're supposed to keep the rest of Congress informed about what the rest of Congress needs to be informed about. And there are questions out there about whether that part of it works as effectively as it should.

MR. OLSEN: I mean, I had some experience with that. I saw very effective efforts by the intelligence committees to make sure that the rest of the Congress was informed, to, you know, establish briefings, you know, and bring us in as members of the executive branch to brief all of Congress. But I also saw what I think is – you know, to your point on the stress on the system, I saw members of Congress, for example, say I don't take classified briefings. And that makes it pretty hard, despite making efforts to inform members of Congress about the nature of activities that are taking place by intelligence agencies if they refuse to accept classified briefings. And the system doesn't work very well if you have that.

So I do think there needs to be – and I think we've seen in the last few years the need for more effective efforts within Congress to understand what's happening outside of just the intelligence committees, which are well informed, by all of Congress. So, to be honest, if not only – it protects the American people, obviously, as the representatives of – you know, as Congress is representative of the American people, but it protects the intelligence community as well, which is looking to have Congress know what's happening so that – you know, that there's that protection by having exposed that information to the Congress.

MS. NAKASHIMA: You know, one of the best examples of that was maybe the bulk collection metadata program by NSA, the Section 215 of the Patriot Act, which was initially started after 9/11 by the Bush administration without any authorization or even congressional oversight. Eventually, got put in under congressional oversight but was restricted in a sense, initially what – correct me if I'm wrong, Matt, all right?

But to the intelligence committees who knew about Section 215? And yet, with the Obama administration coming in, they made a decision that they wanted to, I guess, brief the fuller Congress on this program because it needed to be reauthorized. And, at that point in time, there was an issue I think in terms of just how well Congress was informed of what Section 215 meant, how the bulk collection was authorized under this statute of the Patriot Act that required relevance to an authorized investigation to collect any tangible thing.

MR. KLEIN: Just to be clear, the government was collecting empty records, not the content but the records, of every phone call placed on major carriers in the United States. So with no individualized suspicion whatsoever. Who called who, how long they talked for, et cetera, and putting this into a massive database. And this was under a statute that said that you could get records that were relevant to an authorized terrorism investigation. So there's a quite reasonable argument there that was this was vastly larger than any member of the public would have understood it to be based on what the law said.

MS. GOITEIN: And to be clear also, the information that was made available to Congress under the Obama administration was a fairly short memo, not sort of the actual – not the FISA court opinion on this and not – just a fairly short memo which was eventually released and was surprisingly understated about what was happening and some of the problems that had been experienced in implementing it. Those were delivered to the intelligence committees. The intelligence committees were asked to make it more widely available, especially on the House side. That did not really happen in any meaningful way. So this was not an example of that system of distributing things through the intelligence committees working very well, even though sometimes I'm sure it does.

MR. OLSEN: I just have to – this has been recounted a lot, this issue about the bulk data collection and what was told to Congress. And there's lots of information out there about it, but for my part, I can speak personally, I was involved in attending briefings – this is pre-Snowden – for all members of Congress but they were all invited to come and here – and ask any question and talk anything they needed to know about 215.

So I sort of take issue with the idea that there wasn't any opportunity for members of Congress to know exactly how Section 215 was being interpreted and how it was being implemented.

MS. NAKASHIMA: Some of them didn't avail themselves of the opportunity.

MS. GOITEIN: Well, some of them couldn't. Some of them didn't have the available classified staff available, and that's another problem. It's the way that –

MR. OLSEN: That's an issue maybe with staff.

MS. GOITEIN: Sorry – cleared staff. Staff clearance is a huge issue when it comes to access to this kind of information on the part of a lot of members who are not on the Intelligence Committee or the Foreign Affairs Committee or the Judiciary.

MS. CORDERO: If I can just add a little bit just to kind of – to make a bigger point that I think comes off of what the 215 debate then led to, which then it led to legislation, which is known as the USA Freedom Act, which changed how that collection program worked and mandated more information being publicly available regarding the court, the Foreign Intelligence

Surveillance court's consideration of those types of issues so issues that are larger in scope or that are novel under the law.

And so what I think that experience did is it did change the expectations regarding not only what would be available to Congress but what would be available to the public and to scholars and researchers who follow this area of law and policy. And it really did move us forward – the national security community forward in terms of the transparency that's provided regarding legal opinions and intelligence community efforts to be more public about how their oversight works, what the legal authorities are and how they're implemented. That's still a work in progress, but I do think that the debate over that program that you were describing had ended up moving us forward on the transparency front.

MS. NAKASHIMA: Indeed. Yeah.

MS. GOITEIN: But really quickly, just on this question of the effectiveness of secret oversight, it is notable that USA – that whole debate on USA Freedom did not happen as a result of the 2009 notification of Congress in classified briefings of bulk collection. It happened after Edward Snowden revealed this program to the public. Once the public knew about the program, then there was debate and change.

MS. NAKASHIMA: So you just teed up the next question, which is a proposition and maybe hopefully Ben will come in on this too, but, in practice – agree or disagree – in practice, whistleblowers or leakers and leakers are a vital check on government surveillance powers, Edward Snowden and the bulk collection program being the marquis example.

MS. GOITEIN: Why don't I let someone else go first?

MS. NAKASHIMA: Go ahead.

MR. OLSEN: It's complicated. It's complicated. (Laughter.) So, you know, yes. You know, as a general proposition whistleblowers serve an important, vital role in keeping the government honest. You know, I think that's a proposition that I can agree with. And I think it's more complicated when you look at individual whistleblowers, individual leakers. You know, some are – you know, some have served an important role over the years in exposing government abuses and excesses. The deputy director of the FBI, who is Mark Felt, who was Deep Throat, is one of the more famous whistleblowers or leakers in history and made a significant impact, and I think in a positive way.

I think, you know, there are others – I think, you know, they leak for various reasons, right? So there's an FBI contractor at Quantico who leaked information about a bomb sent by al Qaeda to blow up an airplane. So that was – you know, he's serving a long sentence for that leak.

MS. NAKASHIMA: Yes. In terms of surveillance powers –

MR. OLSEN: So I think it's important to distinguish, you know, what people's motives are and under what circumstances they are leaking. And I think that – I think – you know, I don't think we necessarily want to have the debate in this room about Snowden, you know, traitor or hero, like that's an old – and I'm tired of having that conversation, to be honest.

BEN WIZNER: Did someone call? (Laughter.)

MR. OLSEN: Ben is here. Just in time. We're having this discussion about leakers. So, anyway, I think it's complicated. I think – but I think we ought to look at the individuals and what the circumstances are around the information they've leaked.

MR. KLEIN: So the question is are leakers in practice a key check on surveillance powers? And if so, how do they fit into that broader way we review these things as a society?

MS. GOITEIN: If you would like to take a minute to catch your breath, I can just go for a couple of minutes.

MR. WIZNER: No. I'm sorry. That's okay?

MS. GOITEIN: Okay.

MR. WIZNER: So a few weeks ago, I was on a panel with David Sanger from the "New York Times" and he was describing to the audience at Columbia University how – you know, when he's away from his phone now for 48 hours, he comes back and can't keep track of all the documents that had been leaked to him by people in some parts of the administration.

And he was speaking in particular about early in the administration where we kept reading articles about draft executive orders, the trouble with executive orders, including that the CIA black sites were going to be opened up again. When he would publish articles based on these leaked drafts, there would be a public debate, there would be a pushback, and, more often than not, the executive order would not be published.

And so what you had in those instances was unauthorized leaks to a prominent reporter replacing the interagency process that an ordinary administration would go to before putting out an executive order like that. And his question for the audience was, does anyone want to make an argument that these leaks are not good for democracy, these particular ones, and what would that argument be?

And I guess the way that I would say that in a slightly different way is if we look at the last 15 years, you know, roughly the period in which I've been involved in this work, you know, and we think about what we would not know if the only thing that we knew about national security policy was what executive branch officials officially wanted us to know, we wouldn't have known in 2004 and 2005 about the Bush administration's practice of warrantless NSA surveillance, a story that was broken by Eric Lichtblau and James Risen of the "Times."

Obviously, we wouldn't have known about any of the Snowden revelations, including those that led to substantive reforms.

And outside of surveillance, we might not have ever known that there were black site prisons where CIA prisoners were abused, a whole range of activities were brought to light, allowing reform debates that couldn't have occurred if the public only knew what was within the four corners of what the executive branch wanted us to know.

So there are times where unauthorized leaks are a kind of a safety valve. I think that David Posen at Columbia University has used that term in an article in the "Harvard Law Review." A kind of system response to the problem of over-classification that allows the public to have a debate that it wouldn't otherwise be able to have.

MR. KLEIN: So there's a hidden question though here, which is who decides. Who decides what information needs to come out through that safety valve and what needs to stay secret? So the people's representatives have decided – made one decision and then one individual takes another decision.

Now, on the substance, it's possible that the group could be wrong and the individual could be right. But what is the argument for the individual's right to decide from the perspective of democratic legitimacy, representative government?

MR. WIZNER: So maybe I'll take a crack at that also since I'm late to the table. I think it's a hard argument. I think when you really drill down on the question of who is in the best position to decide, you come up with no good answers. That, you know, saying that the president should decide seems to me illegitimate for a number of reasons, although it has the appeal of –

MS. GOITEIN: Legitimate or illegitimate?

MR. WIZNER: Illegitimate, having been an elected official, but if the president controls the information that we have by which to judge him, and the information that we have by which to decide whether or not to vote for him, that can't be the whole answer to the question. By the same token, you don't want a system where every 20-something-year-old person decides for herself or for himself and substitutes his or her own judgment for the judgment of everybody else.

You know, the least worst way that we've come up with dealing with this problem, as Rumsfeld would say, is to put the media in between the unauthorized disclosure and the public receipt of the knowledge. And so a model in which the leak goes not straight onto the Internet, but to a news organization that exercises some editorial judgment that in cases of national security consults with relevant government officials before publication, should probably, you know, in all instances as you do, I'm sure, doesn't always accept the government's veto request. Sometimes accepts them when it shouldn't, as the "New York Times" did in 2004; sometimes publishes things that the government really wishes that it wouldn't publish.

I don't know that we've come up with a better way than that of trying to manage the – we're talking about two interests here, right? We're not just talking about national security and national defense. We're talking about self-government. And when those two things are in tension, we're going to have only imperfect ways of reaching some kind of balance.

MS. GOITEIN: What I would add to that though is the fact that that system, the system that we've come with, operates extra-legally I think is a problem – a big problem. And I think the fact that our national security – that our laws do not protect national security whistleblowing, I think that system creates a lot of collateral damage, even though it's – we've reached this kind of weird situation where it's – you know, leaks still happen and – it creates collateral damage both in the sense that I think the rules right now for when whistleblowers are protected and when they're not, they're bad rules.

But the alternative to bad rules shouldn't be no rules, right? It should be better rules. And, right now, we're in somewhat of a no-rule situation where I think there is a risk that national security information that should be protected won't be protected, and the baby could get thrown out with the bathwater, let me put it that way. So that's the first concern, collateral damage.

The second collateral damage is people who reveal information that actually has no harm to national security that they do so in order to serve the public interest go to jail. So that's another form of collateral damage from the current system.

And the third, which in some ways is the most important and it's talked about the least is that we end up spending so much time talking about the messenger that we don't talk about the message, which is usually more important. So, I mean, that wasn't the case for bulk collection, but it certainly was the case for Reality Leigh Winner and her leak of information about Russia trying to hack into local election systems.

If you look at the coverage of that, how much more time do we spend talking about this woman, maybe because her name is funny, and, you know, what her fate should be instead of stalking about Russia e-mailing – doing a spear phishing attack on our – I mean, how many people here know how many local election officials had a spear phishing attack? I mean, I happen to know it's 122, because that's what I was focused on, but you all know Reality Winner's name. Is that really – I mean, that's collateral damage, too.

MS. NAKASHIMA: Absolutely. And speaking as a member of a press, we agree that we are struggling at all times to both – to help inform the public, to get at the truth, and, at the same time, protect our sources who are – who speak to us because they feel that there is something important on surveillance, on Russia, Trump, whatever it is, that needs to get out, but yet, you know, we know that they could be, you know, targeted in a leak prosecution. So there is that tension.

I wanted to ask either you, Matt, or you, Carrie, whether you think there should be then some stronger protections where we have to reform this idea of prosecuting national security leakers who leak in the interests of, you know, putting out information they believe is important to the public?

MS. CORDERO: Well, I want to start off though – I'll cover that in a second, but I want to start off just by taking the opportunity to clarify the difference between whistleblowers and leakers because, right now, we are hearing and reading and watching TV discussions all the time about leakers. And leakers and whistleblowers are not necessarily synonymous.

Whistleblowing, not just in the national security context but pertains to individuals who are exposing wrongful or wasteful or wrong behavior or activities that are going on within the government. And there are actually – there are laws that protect whistleblowers. There are channels that are established in government agencies for how individuals even in the intelligence community can report through channels where they do enjoy some protections in order to report to other authorities wrongdoing. And if they are unsatisfied with the process that they can go through within the executive branch, then they can also go to Congress.

Leaking, we are hearing a whole bunch of different descriptions of it and there's a big difference between leaking classified information, in other words an individual who's in a position of trust, who provides classified documents either to a member of the media or to – you know, some website that gets published and leaking what Ben was describing, which is an unclassified draft executive order.

MS. NAKASHIMA: Yeah, but the leak of Section 215 – 215 was classified. The FISA Court order was classified.

MS. CORDERO: Sure. Sure. No, I'm just trying to draw it back a little bit because we're hearing this language used and we're hearing the phrase leakers be politicized in a way that there are differences between each of these individuals, each of these cases, each of the type of information that are being reported.

MR. WIZNER: The law doesn't criminalize the leaking of classified information, right? It criminalizes the leaking of national defense information. And I think it would be hard to argue that a draft executive order about CIA operations wouldn't be national defense information, right? I mean, I think the government would certainly say that it is. Wouldn't the CIA make that argument?

MS. CORDERO: Well, I think the cases that we see that are broad in terms of prosecutions of individuals who are, quote, unquote, "leakers" are leakers of unauthorized disclosures of classified information. Those are the prosecutions that we're seeing. We're not seeing people – and that's why I'm concerned about the political discourse that is accusing former government officials, for example, of being leakers, when they're dealing with unclassified documents that are – the difference being that when a classified document is revealed publicly, then that, by definition, causes some sort of harm to national security.

MS. GOITEIN: Yeah. I would agree. And what you said also touches on another issue with our whistleblowing laws, our whistleblowing protection laws, which there are no statutes that actually protect intelligence community whistleblowers. There are laws that say that they can go to Congress, but those same laws don't actually protect them if they do that. And there's an executive order with a very uncertain future that has some limited protections for limited classes of intelligence officials.

But there are no whistleblowing laws that protect the disclosure of information that has overriding public importance. So it's only information that constitutes evidence of government waste, fraud or abuse or illegal conduct, and that may be necessary. It may be that we need to keep the definition of whistleblowing limited in that way to avoid a free-for-all, but I will say that there are situations where information is – maybe information has been classified that clearly should not have been classified and also, that has no national security ramifications but that is of tremendous public importance, even though it doesn't implicate any sort of government wrongdoing but it's a decision the government made that the public really ought to know about. And we don't have any legal mechanism for getting that out to the public. And I don't know the answer to that.

MR. OLSEN: So just one thought which is to agree with you, Liza, on this sort of pressure valve issue, which I do – I do see there are limitations to the existing whistleblower laws. And from the national security perspective, to the extent we can establish channels for information that somebody in the executive branch is concerned about to provide a mechanism for that person to come forward to Congress, in particular to their own agencies or to others in a different agency, to bring that concern to light is a helpful – is helpful because, ultimately, from my perspective, what we want to do is have that information – you know, have that information looked at by people who are responsible and accountable, but not have it dumped on the Internet.

And as much as I trust you, Ellen, and I do trust you pretty much, not totally, but I do trust you, you know, the reality is that the – you know, the traditional established press is not playing in all cases the gatekeeper role that you talk about, Ben, because I agree with you. That is – that's probably the best system we have for really this problem because we're not going to – (inaudible) – one way or the other because we have conflicting fundamental values at stake. But the reality is that, you know, with WikiLeaks and other sources of being able to put information out in giant dumps, there's nobody playing that gatekeeper role.

And I would say, just in my own experience too that sort of validate the role that you and your colleagues have played, from the executive branch perspective, I've had those conversations with reporters where we've talked about, you know, this is a really important source of information. This is particularly sensitive. Please don't publish that. And I've had, you know, members of the press be very responsive to that.

MR. WIZNER: So let me just make this even harder, and this is a really hard problem. You know, when we think about whistleblowers, we imagine somebody uncovering some hidden episode of misconduct that when it's brought to light in some way, either to a superior high

enough in the chain of command or to a member of a coordinate branch like Congress, action will be taken. But what if the conduct that this government worker stumbles upon is one that has been approved at the highest levels of the executive branch, has been briefed to the intelligence communities in the Congress –

MS. NAKASHIMA: Like Section 215.

MR. WIZNER: And it's been approved by the Foreign Intelligence Surveillance Court –

MS. GOITEIN: Hypothetically.

MR. WIZNER: Pursuant to – right. So I'm just saying that there isn't really some kind of legislative solution to that problem. We're not going to come up with it. So we're going to have to deal with this on the backend in a criminal prosecution for the leak of that national defense information. Are we going to account for the enormous public value, perhaps the weak rationale for having classified it in the first place, can that actually be weighed when we're trying to assess the degree of criminal liability? And the problem is that the current legal regime doesn't distinguish between someone in that situation and someone who sells the same document to the Chinese government.

MS. NAKASHIMA: Right.

MS. GOITEIN: But why did you say we can't deal with that legislatively? I mean, why is the answer not to put either an affirmative defense in the Espionage Act or –

MR. WIZNER: Yeah. Sorry. In that sense. I didn't mean comprehensively you couldn't deal with it legislatively. I mean, it wouldn't be a whistleblower protection law. It would be modifying the criminal law to allow and affirm the defense. Yes.

MS. GOITEIN: Or changing the whistleblower protection laws to include protection against the criminal prosecution, which right now, you know, if you blow the whistle, you can't be – even under the executive order governing the whistleblowing on classified information, you can't be fired but you can be put in jail for 35 years. That doesn't seem like much of a protection.

MS. NAKASHIMA: So the USA Freedom actually had a provision in it for any significant interpretation of FISA to be made public by the court, to be – at least some high-level summary should be made public now. Whether or not that's going to happen we'll have to see going forward but I still remember Jim Clapper, the former – now former director of National Intelligence saying that he thought in the end we should have had a public debate about bulk collection in Section 215. And maybe that would have – before Snowden leaked, and that could have averted the whole mess.

Do you think that our – that the intelligence community now has, you know, learned a lesson or has sort of imbibed that, and maybe culturally has changed to say, if we want to do –

ever do something like this again, rather than do it in secret, you know, in the FISA Court, let's first have a congressional debate.

MR. OLSEN: I mean, one of the – this kind of goes back to the earlier conversation about secret oversight. And I do think one of the – you know, I think it's always evolving. And I do accept that we need to continue to address how we can be better at informing the debate and protecting classified information and protecting our national security.

And I think one of the lines that changed is this idea that interpretations of law would be secret. And I think that that has short of shift. And I think if there's – if you could point to something that's changed, it's that when the government undertakes an interpretation of law, then that should be publicly described and can be publicly described without – you know, without imperiling sources and methods.

And I think that's an evolution over the past few years. That's an important one. And does that release some of the pressure, you know, on this? Maybe, but, you know, going back to he who shall not be named, you know, there are thousands and thousands of other bits of information that have nothing to do with Section 215 that were disclosed about U.S. capabilities around the world that, you know, aren't about interpretations of secret law or interpretations of 215.

And then the other thing I would say is, if I may, what I always come back to when I think about 215 in particular –

MR. KLEIN: Which is the NSA's collection of all the telephone call records of everyone in America basically.

MR. OLSEN: I'm sorry. Right. So this debate was happening within Congress, you know, under the rules that we had been given with people like Senator Wyden, who were very concerned about this interpretation of secret law and he always talked about that. But what he wasn't able to do is to convince his colleagues on the Intelligence Committee that this is something that needed to be disclosed or voted against even, which was the system that was established for having that conversation and having that debate. And he had that debate within his own committee and he was unsuccessful in convincing his colleagues.

MS. GOITEIN: Which goes back to secret oversight because as soon as the public –

MR. WIZNER: Right. But it could not survive public scrutiny.

MR. OLSEN: Public scrutiny in the manner in which it occurred, which was in the very sort of – in my view, sort of inflammatory and sort of skewed debate that occurred in the sort of, you know, spectacular way that this information came to light, which means to me a better course would have been for the government to have anticipated that possibility and had a more rational debate. And I think it might have come out differently.

MR. WIZNER: I guess I wouldn't call a 100-page decision by the Second Circuit Court of Appeals something that occurred in an inflammatory atmosphere.

MR. OLSEN: That's fair.

MR. WIZNER: So you actually had a secret court process where the court heard from one, only the government, ruling for the government, and then an open court process where it heard from us also coming out the other way. And by the time Congress legislated the Freedom Act, more than two years had gone by and there was the kind of debate that probably should have occurred in the first place.

MS. NAKASHIMA: Great.

MS. GOITEIN: So it was really interesting, too, when the director of National Intelligence said, you know, we should have just come out with this information because if we'd done that, then probably the public would have supported it. That right there said to me that it wasn't really classified for overriding national security reasons. He wouldn't say that about the nuclear codes. He said, well, we should have just – he didn't say we should have just released the nuclear codes because then we could – because you don't release nuclear codes. But he was basically saying, you know, we thought the public wouldn't support it, so we didn't release it.

MR. OLSEN: I don't think he was saying that. I do think it's not so black and white as nuclear codes and, you know, sort of your daily schedule. You know, it was a harder call I think on the classification, the legal argument to the extent to which – you know, the argument is – the extent to which a legal argument exposes information that would allow your adversary to avoid, you know, the surveillance basically.

And I do – and that's what I'm kind of saying here is I think that has shifted to the point where legal decisions, legal arguments are – the presumption should be that they can be publicly described without imperiling the source.

MS. NAKASHIMA: Carrie?

MS. CORDERO: So I would just – I think I would add to that by arguing that not only has the recent years' experience over the bulk telephone collection program, over the Snowden disclosures and other leaks of information – not only have they affected decisions about releasing legal opinions, I think what we're going to see going forward is actually a change in the way that the intelligence community and the policy leadership evaluates the actual collection that's going to be done. And I see that for a few reasons.

Number one, I think it's because the nature – first of all, the volume of the information that is collected is very different from the late '70s, the '80s, the '90s in terms of the way that everybody communicates and the differences and the privacy implications of that, so the volume of communications that are potentially collectable under these authorities have changed, the nature of the information – the texting, the e-mails, you know, different chat apps, all these sorts

of different modes of communication that are exploding every single day are changing the nature of what surveillance can potentially obtain.

And, two, the risks are different now in an environment of incredible volumes of information being leaked and because of the risk of cyberattacks or hacking of potential information. So the risks of doing certain types of surveillance activities are also now – vary greater and vary differently certainly from the time when I was handling foreign intelligence surveillance matters in the mid-2000s even.

MS. NAKASHIMA: So that actually is a great lead-up to the next proposition which is: agree or disagree, it is inherently dangerous for the government to store large volumes of Americans' electronic communications in searchable databases, such as the old Section 215 bulk collection, the metadata database.

MS. CORDERO: So I'll start off and then tee it back up because that is – I mean, that's sort of what I was getting at –

MS. NAKASHIMA: Exactly. Yeah.

MS. CORDERO: I can't agree or disagree, but I think that the risks are different than they were certainly in 1978 when surveillance, we were just dealing with phone types of communications as that – as the technologies evolved and the surveillance what it was targeting changed.

I think the risks are different now. And I do think that there have been leaks, for example, we've seen public reporting regarding leaks of sensitive NSA technologies and how the NSA does its work. These types of leaks put a greater burden on the government to provide assurances that if it's going to collect certain kinds of information, it better be able to protect those types of information.

So I think it changes the risk analysis and I think it also changes the burden on the government to demonstrate its ability to protect information if it's going to go ahead and collect it under lawful authorities and for valid national security purposes.

MS. NAKASHIMA: Ben?

MR. WIZNER: Yeah. So in 1978, the cost of storing one gigabyte of data would have been well over $100,000 and now it's pennies. And so it really is fundamentally a different world. Where once privacy protection that we enjoyed historically was created by the cost of collection and storage, now those costs have become so trivial that it's very easy for – and we'll get to the corporations as well but for governments to amass and not delete, huge amounts of information that would have been impractical to do a long time ago.

So there's different kinds of risks that that creates. I don't think anybody would say it's not dangerous. We're certainly learning in the last days that, you know, one of those dangers is

if you don't protect those databases, some of the things that you're holding could end up in the hands of people who want to do a lot of mischief with it.

And I just want to focus briefly on a different kind of democratic danger here, which you might describe as mission creep. And I would say something like this, that when and if there is a significant terrorist attack in the United States, it's overwhelmingly likely that evidence that would have prevented that attack will be sitting somewhere in an intelligence community database. And that's because if you collect and store all of these dots, they're going to connect in hindsight.

I hate the argument that that means that the intelligence community made a mistake. The world looks very different when you're looking forwards or when you're looking backwards. And we need to change the politics around blame when there's a terrorist attack.

What I worry about, though, is that this will be an opportunity for people in government to say, but for your rules about what we're allowed to query and what we're not allowed to query, we would have been able to find the evidence that would have stopped this attack. And so the current regime under which this was collected for very narrow purposes and can only be viewed a few hundred times a year is going to be opened up. And this information is going to be made available to criminal investigators and to – more or less what we saw with the Patriot Act after 9/11, which tore down the wall between criminal and intelligence investigations, that we're going to open up these boxes that, you know, have been collected for anti-terrorism purposes and used them for a broad range of purposes.

MS. NAKASHIMA: Let me just ask you, though, if that information had been in a government database – and it might not have. It might have been sitting in a company's database, but if it had, would you not have wanted to stop the attack?

MR. WIZNER: I mean, that's a crazy question. (Laughter.)

MS. GOITEIN: Respectfully.

MR. WIZNER: I'm not that (respectful ?). Yeah. Oh, you're saying respectfully. Yeah. Okay. Then I respect it back. I would have wanted to stop the attack.

MS. NAKASHIMA: Okay.

MR. WIZNER: What I'm saying is that, you know, again, the dots always connect in hindsight. You know, the fact that information is residing in a government database does not mean the government should have stopped the attack. And it doesn't mean that the government would have stopped the attack if there had been no rules on what they could look at.

The number of possibilities in the future is infinite. When you're looking backwards, you were trying to put together the pieces on one event. So, you know, I reject the notion that it was because there was this handcuffing that we didn't stop it. In almost all of the Western terrorist

attacks that we've seen in the last few years, the attackers were known to investigators. You just cannot create an expectation that we're going to stop every terrorist attack.

MR. OLSEN: Can I just very quickly – because that's a great moment to agree with you, Ben, really. And the politics of blame is a real problem for the intelligence community. And it does mean that the importance is to really make these decisions now, not in the aftermath of an attack, to try to get this right, to understand what the government should have access to, what it shouldn't have access to.

And, just very quickly, right after Boston Marathon attacks, there was this idea that, you know, because we had some information about the Tsarnaev brothers, right, the two guys responsible, that the FBI had a minimal amount of information, that everyone in Congress, it didn't matter, left, right, Democrat, Republican was why didn't you, you know, arrest that person or have surveillance on that person 24/7 on that person. And it was based on a tip from the Russians, right?

That's all about all we had was a sort of – and so it is – I agree with you that the politics of blame create all kinds of bad incentives and we need to get this right before the attack.

MS. GOITEIN: Yeah. And I was just going to sort of pile on to your point about mission creep, which I think is a major risk. And the way it always works is that in the beginning, when the government is proposing to do more collection than it did before, new collecting things, new big databases and people are nervous, the government says, don't worry. We'll have these very stringent limits on how we use it. You can rely on those limits and that will protect you.

And then, as soon – and then, a couple of years later, the policy changes, they want to get rid of those limits and then when people say, but those limits were what were protecting us, they say some version of – I can give you a specific example after I tell you this, but some version of, you know, well, once we've collected it, we can use it for any lawful purpose or don't you want us to prevent the terrorist attack? We need to share information.

And so it goes very swiftly from you don't have to worry about all this collection because we have these protections on the backend to those protections on the backend are inhibiting information-sharing and inhibiting our ability to protect you. So you just need to assume in the beginning that whatever is collected will eventually be available for any purpose and evaluate collection programs on that basis. And this is happening as we speak in the context of Americans' communications that are incidentally collected when the government targets foreigners overseas for foreign intelligence surveillance.

And, originally, the argument was you don't have to worry about this incidental collection because we'll have very, very strong backend protections. Those protections originally included a prohibition in the agency's rules against the agency's sorting through the data looking for Americans' communications. They've now gotten rid of that rule, and they've

said, well, we collected it lawfully. We can use it for any purpose we want. And even if that weren't true, don't you want us to catch the criminals?

MR. KLEIN: So we've talked about the powers that the government has, we've talked about what we want the government to achieve. I'd like to talk a little bit now about what we're afraid it might do. Every child has the boogieman who lives in the closet or the monster that lives under the bed. And for those of us who work in this space on surveillance policy and law, the monster under the bed is – and I apologize if we have any retired FBI agents here – J. Edgar Hoover.

And, as we all know, J. Edgar Hoover kept files on politicians, on civil rights leaders, on activists, on people like Martin Luther King Jr. And then he deployed those files pretty aggressively to bend politicians to his will, to secure his own job security, to try to push people out of public life.

Judge Silverman, the D.C. Circuit legendary figure, who's held jobs in all the different branches of government, had to review the J. Edgar Hoover secret files after Hoover died. And he said it was the worst experience of his professional life. And if you know Judge Silverman, he's not a shrinking violet. Must have been some pretty awful stuff in there.

And so the question for our panel is, could it happen again? Could we have another J. Edgar Hoover? And if yes, if you think it could happen again here, how would we know that it's happening?

MS. CORDERO: So I'll start and maybe we'll go around. So many of us who work in this space or have experience in this space with regard to surveillance that's conducted specifically under the Foreign Intelligence Surveillance Act, which is the act that governs collection here in the United States for foreign intelligence purposes, our national security purposes, and then also there's other authorities that govern certain communications that are collected against non-U.S. persons outside the United States.

But this set of collection activities that occurs under the FISA, the Foreign Intelligence Surveillance Act, I would suggest is probably the most highly regulated and highly oversight-laden environment in government national security related space. So we have a court. There's a lot of procedures that take place. There's oversight by the Justice Department and the director of National Intelligence. There's a fairly – there's a robust and institutionalized process for oversight.

But there's other things that go on in the government. And the FBI operates – I would also sort of – I worked a lot with the FBI when I was in government, and the FBI also has attorney general guidelines that they operate under that govern all of their investigations. So it does matter sort of whether the attorney general would potentially change those guidelines. There's one opportunity for there to be change, but the FBI will follow what guidelines the attorney general sets, and there's an inspector general of the Justice Department.

So FBI, Justice Department, intelligence community, I feel like based on the experience that I had in the past that there are a lot of oversight mechanisms. I think there are potentially other areas of government – Department of Homeland Security. I know Secretary Kelly is going to be here later today – where there are a lot of investigative activities and potential opportunities for a lot of collection of information about Americans that is worth looking at in consideration as to whether or not there are oversight structures and accountability that exists the same way that I know some of the surveillance regime operates.

So I think, from my perspective, at least based on my government experience, I think there's a lot of confidence that can be given for sort of this very specific FISA-related surveillance, but I think there are other areas that are in the national security or homeland security space that are certainly worth those folks who work in this space thinking about and following to make sure that other areas of government that may now take a more aggressive role, particularly in domestic law enforcement activities, are held to the same high standard.

MR. OLSEN: Well, I'll jump in. I think that is a good question to ask – could we have another J. Edgar Hoover, could we face that kind of sort of abuse of power. And, you know, as Americans, this is something that is sort of our birthright is to be distrustful of power, especially when it's, you know, aggregated in one place and unchecked.

And as a practitioner of national security operations and law – and I've looked at ways to check that kind of power, it seems to me one way is to sort of imagine the worst-case scenario and then write laws and rules to stop that worst-case scenario. And that's what I've seen when that impulse takes hold is, you know, restrictions on activities that we want the government to engage in. You know, so you can imagine the worst-case scenario and try to stop – you know, write laws to stop that and you end up really undermining our national security.

So the way I've thought about how to check that type of power is through strong institutions, and in particular separating powers, which is, you know, our founders' great insight, and that means independent judiciary, legislative oversight, and a strong press. And as long as we respect and strengthen those institutions, then I think we're in good shape. When we denigrate those institutions, when we take shots at those institutions and weaken them, then the possibility – the potential for power to be amassed and abused is greater.

MS. GOITEIN: Gosh, there's a lot in this question. First of all, I want to say it wasn't just J. Edgar Hoover. I mean, we can't hold him up as this aberration. The Church Committee looked into this and found that presidents – every president and members of those presidents' administration from the inception of the national – or the national security and surveillance state through to Nixon had abused these surveillance authorities to go after their political opponents.

It's not J. Edgar Hoover. It's human nature. That's why we have the laws we have and the institutions we have. So power will be abused if power can be abused. So then we have the institutions. But I would add to what Matt said. I think the substantive laws are important as well. I think the greatest check that we have had on political abuse of these powers has been the principle that's been enshrined in a variety of different laws and policies, again, after the Church

Committee, that the government should be not be able to collect Americans' information unless it has individualized fact-based suspicion of wrongdoing. And that's what we had that was incorporated into FISA. It was incorporated into attorney general guidelines. It was incorporated into a number of different policies.

Since 9/11, that principle has been stripped out of those laws fairly systematically, so whether it's FISA or with Section 702 or national security letters or – which is a sort of administrative subpoena to get some kind of business records or Section 215 we were talking about earlier with the telephone records or the policy for searching electronic devices at the border or the – in any way you look, the permission to gather Americans' information without individualized suspicion of wrongdoing has been greatly expanded. I think that – I worry about that just as much as I worry about what I also see happening to the institutions, which I think are in their own way under attack.

I think, right now, we are heavily reliant on a culture of compliance in these agencies. That culture of compliance was a result, kind of sprang up over time as a result of the institutions and laws that were put in place after the Church Committee. As those institutions and laws become weakened, you know, systematically, I worry very much about what will – about the culture could follow because we're relying on that very heavily now.

MR. WIZNER: So I'll be very brief on this one. There was a very interesting exchange in a Senate hearing yesterday where Senator Lindsey Graham was adamantly insisting that the intelligence community disclose to him whether it had recorded conversations that he had had with foreign leaders and was getting increasingly frustrated when he wasn't getting a straight answer.

I don't think that what Senator Graham was suggesting was that he was being personally targeted for surveillance. I think he was reflecting what might be the dangers of more or less passive collections systems that just by routine and by design collect all kinds of information.

Now, in Hoover's era, he needed teams of agents to assemble these dossiers, and now, for every single person in this room – and I would include every member of Congress and every judge – there is somewhere a database of ruin, a collection of information that was not in any targeted way amassed and combined about that person, the release of which would cause tremendous harm.

So we just have a different risk environment because of technology. And we're seeing some of this when there's a hack or when there's a leak and people's lives get turned upside down, even if they weren't personally targeted here.

I'm surprised that no one has, you know, said the name Trump in response to this question, but I will admit that, you know, given that environment, with so much information sitting in private and government databases, I was very nervous at some of the names that were being considered for attorney general and FBI director in Trump-land. It did actually make me think that we could go back to an earlier era of abuses.

MS. NAKASHIMA: So your mention of the big data bases that could contain sensitive information that are being amassed not only by the government but also by companies like Google and Facebook brings me to the question, which is the bigger threat to Americans' privacy? Government surveillance or companies like Google and Facebook?

MR. KLEIN: Or being hacked by a foreign intelligence service and have your stuff put online.

MS. NAKASHIMA: Yeah. Right.

MR. WIZNER: I think, you know, one of the answers that I sometimes give to this question is that we're looking at different threats from these entities. At least at this point, Google and Facebook can't deprive us of liberty or life, which is something that government can, and so there's a different kind of coercive authority that can be brought to bear.

But, actually, briefly I think I want to focus on a real similarity. I think we ask the word privacy to do a lot of work in this kind of question, but we're really concerned about a lot of different things. And one of them is about power and abuse of aggregated information and fairness. You know, what happens when institutions, whether they're corporations or whether they're governments, have a lot of information about us that they're processing in secret and making decisions about us that are not transparent and that affect us that are not easy to challenge.

And so one example of that that people will have encountered is a mistake on a credit score and this sort of byzantine process for trying to get that fixed. And even understanding how that might have come about. And I think that one of my concerns going forward is that we're moving more and more towards a world of scoring, where, again, very important decisions will be made about – that affect whether we can get a job, whether we can get bail, what line we're in at the airport – that combine private information and government information, where, for various reasons, some involving national security, some involving trade secrets, we're not able to get the kind of due process that we'd expect when these kinds of decisions are being made about us.

MR. OLSEN: I think it's scary that you said that, you know, Google and Facebook don't have the power to take away our life and liberty yet. (Laughter.) So I noticed that. Maybe you know something we don't.

So I basically agree. You know, you look at the amount of information that's being collected. And I think the one – the difference right now that I focus on that makes the government in some ways more of a concern is the ability to act on the information because in comparison, the amount of information that's collected about us by private companies is far greater. And then you look not really into the future, and you think of, like, you know, digital assistant devices in our homes, you know, like Alexa and Siri or smart televisions that are always on, recording – you know, recording all of our conversations in our homes and it's – you know – and I worry about that.

And I think, you know, all that information, that it does – I think you're right to say privacy does a lot of work in these conversations. You've got to really focus on what you mean when you talk about privacy, because we've relinquished so much privacy to private companies. And, you know, having worked in the government, it really doesn't – there's nothing in government that compares to what is collected by private companies. The difference right now is the way that information can be used, you know, in problematic ways.

MS. GOITEIN: Although a lot of what civil liberties advocates worry about with companies gathering all this private data is that that data can become at least theoretically available to the government, whether the companies are voluntarily providing it or whether they can be compelled to provide it. It's true. The government doesn't necessarily go in and try to get all of it but it can get what it's interested in. And so the distinction between the two is not necessarily that clear.

And I also think – you know, as a civil liberties advocate, I am always thinking about the government and proper limitations on the government and what the government can do to people. And so, you know, that's my mindset. I'm paid to worry about that so I worry about that much more than I worry about what companies are doing. And for the most part, if I think about it, you know, companies don't have the same incentive necessarily to persecute people because of their ideologies or their political ideologies.

But as I think about it, it is certainly – companies have their own financial incentives to prefer some policies over other – social or economic policies that can benefit the bottom line of a company significantly, and that an give a company the same kind of incentive to mess with people who might be kind of standing in the way. And it's not that they're going to put them in jail, because they can't, but they can mess with their credit score, right? I mean, there are various things that – or they can, you know, kind of mess with the lives of, you know, members of unions or that kind of thing.

So I am not at all sanguine that companies couldn't at some point pose the same kinds of threats we worry about from government.

MS. NAKASHIMA: Carrie?

MS. CORDERO: I would just add that now, especially because even though I was in the past in the government but now I'm with a law firm that represents not those specific companies but companies that are in the communications space and technology companies that retain data, is that certainly the last few years the – (inaudible) – the last few years and the concerns about government surveillance obviously affected the companies and have change their behavior, have actually had an impact on both their relationship with their customers and how they actually handled data.

So I think we have seen in recent years changes that the companies have made in response to the privacy concerns that have been expressed more about government surveillance.

MS. NAKASHIMA: Post-Snowden especially.

MS. CORDERO: Right, but the way that companies interact and the way that the companies think about handling the data. And also, king of bringing us back to where we started the conversation in terms of another level of oversight that we're seeing, really comes into play with respect to the legal avenues that companies have if they are on the receiving end of a government request for data that they deem to be not lawful or not consistent with the statute.

We are seeing more cases of the case that Microsoft has brought in the Second Circuit that some people have referred to as the Microsoft Ireland case but this is about a government request for information, for data stored on a server in Ireland. And so it was a different interpretation of a privacy statute that concerns when companies can give information to the government.

And so this is an example of a case where the courts are serving as perhaps more of an instrument of oversight if you want to define oversight really broadly as a restraint on some type of government ability to obtain data. The courts are another avenue that we're seeing I think play more of a role going forward.

MR. WIZNER: One quick point about the courts is there's a very important Supreme Court case this fall that's not getting the same amount of attention as the Muslim ban and others. And it has to do with whether law enforcement has to obtain a warrant before going to telephone companies and obtaining your historical cell phone location information.

And at the center of it is a Fourth Amendment doctrine that provides that if you share your personal data or information with a third party, one of these companies, you have waived constitutional privacy interests in that data. And in the digital age, where we really share our entire lives with platforms that are controlled by private companies, that's a very odd doctrine which is going to be in the crosshairs of the Supreme Court this fall. The case is called "Carpenter vs. the United States." It's an ACLU case.

MR. KLEIN: That's a great forward-looking note to end on. It's the CNAS tradition to try to finish close to on time so I'm going to close with that. As an American who cares about being safe and being free, I'm glad we have all four of our panelists on the – (inaudible) – as it were, defending both of those important values. Please join me in saying thank you to them. (Applause.)

End Transcript