# A New Paradigm of Leaking

Alex Abdo, David Cole, George Ellard, Kenneth Wainstein,
and Stephen I. Vladeck*

*This panel featured a discussion surrounding whether or not episodes like the Edward Snowden affair suggest that the U.S. government is experiencing a "New Age" of leaks and, if so, the ways in which the act of leaking classified information has changed. In addition, in light of the debate surrounding the constitutionality of the NSA's surveillance programs under section 215 of the USA PATRIOT Act and section 702 of FISA as added by the FISA Amendments Act of 2008, the panelists discussed ways in which those who work for the government legally may express their concerns without resorting to leaks.*

Introduction: I would like to introduce the third panel that we have joining us this afternoon, which is going to be discussing a new paradigm of leaking. Among our panelists we have Mr. Alex Abdo, who has been a staff attorney with the ACLU National Security Project. He has also been involved in litigation of cases concerning the Patriot Act, Foreign Intelligence Surveillance Act, International Emergency Economic Powers Act and the treatment of detainees in Guantanamo Bay, Afghanistan, Iraq and the Navy Brig in South Carolina. We also have Professor David Cole, who is a professor of law here at Georgetown University. He specializes in constitutional law, national security law and criminal justice. Professor Cole has litigated many significant constitutional cases in front of the Supreme Court and has been called one of the country's great legal voices of civil liberties today and a one-man committee of correspondence in the tradition of patriot Sam Adams himself. We also have Dr. George Ellard, who is the Inspector General of the U.S. National Security Agency. He served as counsel in the congressional inquiry into the terrorist attacks of September 11 and was responsible for drafting classified and public reports that recommended transformational changes in the structure of intelligence and law enforcement communities today. We also have Kenneth Wainstein, who is the chair of Cadwalader's Business Fraud Group. Mr. Wainstein previously served as the First Assistant Attorney General for national security at the Department of Justice under President George W. Bush. And finally, we have Professor Stephen Vladeck, who will be moderating this final panel. Professor Vladeck is a professor of law and associate dean at American University Washington College of Law and is nationally recognized for his expertise in constitutional law and the role of federal courts in the war on terrorism and was part of the legal team that successfully challenged the Bush administration's use

* What follows is an edited transcript of a panel entitled "A New Paradigm of Leaking," held as part of the *Journal of National Security Law & Policy*'s February 25, 2014 symposium on "Leakers, Whistleblowers and Traitors: An Evolving Paradigm."

of military tribunals at Guantánamo Bay in Cuba. So in this panel today we are going to be exploring the extent to which a new paradigm of leaking does exist and how the law today may adapt to account for that.

Stephen Vladeck: Thank you! The title of our panel is A New Paradigm of Leaking. I think there is a missing question mark, because one of the questions I hope we'll start with is whether, in fact, there *is* a new paradigm of leaking – that is to say, have the national security leaks of the past several years, the leaks by Bradley/Chelsea Manning, the leaks by Edward Snowden, have they really been different in kind from national security leaks of the past, or is it mostly a difference in degree? If it is a difference in kind, what does that mean, what should that tell us going forward? Indeed, as we're trying to figure out where law and policy should end up with regard to national security leaks, understanding what's new and different about the latest developments, is a fairly important piece of the conversation. So with that I'm going to ask George to start us off by posing a very general question to him. Is this a new paradigm of leaking, at least from your perspective from the NSA?

George Ellard: Thank you, Steve. I have been with the National Security Agency for almost seven years, this is the first time I have spoken in a public forum, and I must say I approach this with a lot of fear and trembling over the possibility that I might disclose, inadvertently, classified information – because that could have dramatic consequences. Since the initial leaks by Mr. Snowden, the director of national intelligence, the director of the National Security Agency, and many other highly placed people within the U.S. intelligence community have asserted that Mr. Snowden has done long term and irreversible, negative impact to our national security. They asserted that he has damaged the intelligence community's ability to keep our country safe, that he has put the lives of Americans at risk, and that he has helped terrorists whose aim is to kill us. I do not think that these assertions are hyperbolic. And I would like to start out by first giving you some idea of what Mr. Snowden has done, and then compare him to another – I hesitate to call Snowden a spy – but another person who indeed was a spy about whom I happen to know something. Several years ago I read an article in *Der Spiegel*, the German equivalent to *Time* magazine or *Newsweek*, and the article reported that the NSA was able to, so to speak, tap into the communications of senior Al Qaeda leadership including Osama Bin Laden.[1] The article went on to explain that these terrorists believe that if an e-mail were not sent, the NSA would not be able to catch it. So Osama Bin Laden, according to *Spiegel*, would type up his instructions to his agents and save the message file – the message – in the draft folder. His agents knew his password – Osama's password – and they would go into his account, look in the draft folder, respond as well, and save the draft. Nary an e-mail was sent. And as a consequence of, according to *Spiegel*, our ability to tap into Osama's

1. Hans Hoyng and Georg Masolo, *NSA Surveillance: Eavesdropping on America*, DER SPIEGEL, May 15, 2006.

account, we were able to thwart several dangerous terrorist plots. Now I'm not going to comment on the accuracy of the *Spiegel* report, but I can tell you one thing: if the NSA were able to tap into the communications of senior Taliban or Bin Laden associates the day before the *Spiegel* report was issued, we could not do it the day after. Our adversaries are very sophisticated, particularly in the IT realm. They do not live in caves in Afghanistan, and they read *Spiegel* and the *New York Times* and *Washington Post* and the *Guardian*. I think – at least to the degree I can explain it today in this open forum – that Mr. Snowden has done two kinds of harm. First of all, he has revealed particular weapons that our intelligence community had been using to protect our security. Once they are made public, we lose them. Secondly, he's revealed a great deal of stuff, a great deal of information about NSA's current strategic posture and how it intended to proceed in the future. All of that is lost. In deciding whether Snowden and Private Manning are exhibits of a new paradigm of leaking, I would like to briefly contrast and compare Mr. Snowden – I know very little about Private Manning – with another person who leaked an incredible amount of classified information: then-supervisory special agent Robert Hanssen of the FBI. A presidential commission declared that Hanssen had perpetrated, and I quote, probably the worst intelligence disaster in U.S. history. In the sentencing memorandum, federal prosecutors described Hanssen's crimes as surprisingly evil and almost beyond comprehension.[2] Hanssen had a career of over 23 years during which he gave, first of all to Soviet and then later to Russian elements, just reams of information and dozens of computer diskettes, containing, according to the presidential commission, national security information of incalculable value. I'll give you an example. Hanssen compromised a plan that the U.S. had developed to protect its military and political command in the event of a first strike by the Soviet Union, and he did that at a time when key elements within the Soviet oligarchy were advocating a first strike against the United States fearing that America would take advantage of the then-crumbling Communist empire to launch its own preemptive strike. So Hanssen stands, I thought until last year, alone in the damage that he has done to our country and to our national security. And Hanssen and Snowden were alike in that they both used really well-honed IT abilities to steal and disclose classified information vital to our national security. But I think the comparison ends there, and I think perhaps that Snowden and Private Manning really do exhibit, or are exemplars of, a new paradigm. Hanssen's motives were venal, for cash perhaps, or perhaps there were psychological: a desire to play in a very, very dangerous game that is therefore very, very exciting. At the end of his career Hanssen had almost 30 years in intelligence and counter-intelligence. He knew exactly what was of value to his spy handlers and he was very specific in choosing documents to steal. He knew how to control his handlers better than they knew how to control

2. COMMISSION FOR THE REVIEW OF FBI SECURITY PROGRAMS (Mar. 31, 2002), *available at* http://fas.org/irp/agency/doj/fbi/websterreport.html.

him. Snowden, in contrast, was manic in his thievery, which was exponentially larger than Hanssen's. Hanssen's stuff was, in a sense, finite, whereas Snowden is open-ended as his agents decide daily which documents to disclose. Snowden has no background in intelligence and is likely unaware of the significance of the documents he stole. In contrast to Hanssen, Snowden's apparent confidence that he could control others who were interested in those documents for whatever reasons is to me astonishing naïve, ignorant and egotistical. In sum, if there is a new paradigm in Snowden's treachery – and for that matter Private Manning's – it is of young, inexperienced, unknowledgeable people claiming to act out of noble intentions, making sweeping collections of material vital to the national security and transferring possession of that material to other parties who control its distribution.

SV: So I guess it begs the question, because in describing the damage caused by the disclosures, I'm reminded obviously of the *Chicago Tribune* episode from World War II. And the front-page story about how we won the battle of Midway because we had broken the Japanese naval codes, which appeared in the *Chicago Tribune* that, fortunately, the Japanese Navy apparently didn't read.[3] And I guess what strikes me about the analogy . . . it seems to me there have long been incredibly damaging international security disclosures about the communication intelligence capabilities of the United States. Is it the naiveté of the leaker that is different in the current cases? Is it the volume of data we're talking about with regard to the *Chicago Tribune* episode? We're talking about one specific item which was one specific intelligence capability, although a pretty big one at that. Aren't things different today? If so, are they different in a way that requires different reactions?

Ken Wainstein: That's a good question. First I just want to say I think George's articulation of that position is one of the best I've ever heard. You really captured, I think, the danger that the Snowdens of the world present to national security. In terms of what's different about the Snowden/Manning leaks and what we've had in the past, they are different in a variety of ways. Whether there is a new paradigm or not, I think these are just sort of examples of different dimensions of the same problem. You take a look at the *Chicago Tribune* leak and that's sort of the iconic leak that people like myself trot out whenever we go in front of Congress to justify the fact that we have laws that make leaking illegal – because it's such a great example. Here we have this incredible advantage in the war against the Japanese, i.e., we've broken their military code, and that fact gets leaked, and if the Japanese had picked up on it, it could have resulted in the additional deaths of literally hundreds of thousands if not millions of people if they had taken different defensive measures and possibly made us invade Japan. So, it's a great way of showing the implications

3. *See* Gabriel Schoenfeld, *Has the* New York Times *Violated the Espionage Act?*, COMMENTARY, Mar. 1, 2006.

of these leaks and, therefore, justifying the need to prosecute leakers – that the danger is real, it's not just fanciful. And sometimes that's a problem. People say, well, gosh this leak happened – and we've heard this a lot over the last year: this leak happened, but the sky didn't fall, we haven't been struck by a terrorist attack, we haven't been invaded, an ICBM hasn't hit the Capitol. That is because it is hard to see what the damage is, and that's why I think George's articulation is very good because that damage is real. In the background the intelligence community, the military is trying to account for it. It's real, in terms of the damage to our readiness and the damage to our ability to protect ourselves. But I think, in terms of at least seeing something different about the WikiLeaks, Snowden leaks and things we've had in the past, one is obviously the volume. Two, it's the intention, which is what George is pointing out. With WikiLeaks, you had [] a whole operation set up and designed to reveal secrets. That raised an issue that you don't see so much in the Snowden situation. That raised the question of, okay, do we prosecute WikiLeaks? And that raised the legal issue of prosecuting the recipients of leaked materials, i.e. Manning's material, as opposed to the leaker, which is what made that issue so interesting from the legal and constitutional perspective because, if you are going to prosecute the recipient, i.e., WikiLeaks, then why not prosecute the *New York Times* the next time it discloses classified information because they are basically on a par? The Snowden leaks similarly show a methodical effort to expose things for the point of exposing them, for whatever idealistic motives. But that's very different from what we had with Hanssen. My concern is, given these two situations happening within a couple of years and the fact that there is some element of sympathy out there for them – and, in fact, some have jumped to lionizing Snowden – that's problematic. I think that if people see that folks can unilaterally decide that they are going to leak information they disagree with and violate their oath, then I think our national security system doesn't work. The oath that we make as government employees doesn't work. And we end up with a much handicapped national security operation. That is why I think it is important, to the extent we are able to bring Snowden to justice, that we do so.

SV: So Alex, Ken mentioned differences with regard to volume and with regard to intention, certainly with regard to WikiLeaks, perhaps also with regard to Snowden. Do you think that's a fair basis for distinguishing recent events from historical ones? How do you approach this question?

Alex Abdo: I think technology certainly may have changed the equation from the government perspective, but I think it's important to ask the antecedent question which is: how is it that leaks on this scale were possible? And I think the only answer to that question is because secrecy has also taken form in that scale. We now live in a world in which there is more classified information than there is unclassified information, and that is an extraordinary state of affairs. And it's not just the kind of secrecy that I think has traditionally been kept secret – when you are talking about intelligent sources and methods, which is

traditionally secrecy relating to intelligence operations – but it's the sort of secrecy that creates a gap in public understanding, a gap between what the government is actually doing and the very basic understanding the public has about the authority that the government possesses. And that gap can be extraordinarily corrosive to a democracy; it can undermine trust in government, which has been one consequence of the public realization of exactly what has been taking place over the last year, last ten years. And I think that level of secrecy persists, at least when it comes to surveillance, for two fairly obvious reasons. One is because surveillance is now possible on such an extraordinary scale that the system of secrecy has ballooned in a sense; and the other is that, in many ways, it's far easier to keep that information secret. For one thing, there is a smaller footprint for these government operations given the use of technology to, you know, automate certain processes or have one person do something whereas you might have needed a group of 20 to do it in years past. And the other, it is far easier to detect leakers. Now that, obviously, for the government was no consolation for Edward Snowden, but in the future, if Professor Sales' recommendations are taken, will be the case. In my mind, the new paradigm is not that leakers have changed so much but that the government can actually exercise ever more powerful authority and keep that ever expanding authority more a lively secret. And that poses a real challenge to democracy – to our democracy – to figure out how to draw the line when the public should be brought into the conversation. And I think one quick related observation is that . . . I came out of the first panel thinking to myself that the whistle blower protection laws as they exist in this country now serve primarily one purpose, which is to allow low level individuals to make sure that senior individuals are aware of what's going on, essentially to make sure that the executive and the Congress more or less understand what's going on, so that if there is something illegal going on, everybody knows about it and can decide whether they want to approve of it. And I don't think that's a sufficient scope to think of whistle blowing. I think Snowden's biggest revelation was not that the NSA is collecting a record of virtually every phone call every day or that the NSA has subverted our best protection to cyber attack – namely encryption – or that the NSA scanned every text message or e-mail going into and out of the country for suspicious key words. I think the biggest revelation is that the compromise that the intelligence agencies made in the 70's to agree to oversight but keep that oversight largely secret has broken down. Our system of checks and balances has broken down. It's not enough to leave to the executive the decision about what information should be public in deciding questions of public policy. There are certain questions that the public needs to be a part of, and I think that's in part a technological change. We now live in an era in which pervasive surveillance is possible, and we need to ask questions and answer questions in a public way about whether we will tolerate that form of surveillance, that extent of surveillance, and I think those basic questions have to be debated publicly.

SV: Someone should write a blog post about the breakdown of the 1978 accommodation.[4] So David, Alex's point was an artful framing of a question I want to ask all of the panelists, but I want to start with David. If technology is responsible in both directions for both the increase in secrecy and the increase in the ability of individual government employees to actually disclose far larger volumes of information that might have been true in the past, does that suggest that this is just a race to the bottom – that no matter what happens in the next six months, we are going to continue to see both an increase in secrecy and therefore an increase in instances and incidents of high profile national security leaks by future Snowdens?

David Cole: I think so. I agree with Alex. The digital age has increased the capabilities on both sides of the aisle. It's increased the capabilities of leakers; no could have photocopied 1.7 million documents and still been alive to release them when he was finished. It's also increased the ability of the government to identify leakers. They caught the guy who leaked the story about the insider on the al Qaeda in the Arabian Peninsula bomb-making team pretty quickly once they got the phone data that they sought, so I think it's increased it on both sides of the aisle.[5] I also think the global reach of digital technology has increased the sort of risks on both sides of the aisle, so the government has now – because digital knows no boundaries – the government has the ability to gather up massive amounts of information that it never before could have imagined around the world. And it gets push-back when it does it to us, but it doesn't get much push-back from us when we do it to them. But at the same time, the leakers of the world can disclose stuff to entities and individuals that are beyond our control – the *Guardian* newspaper or WikiLeaks or Julian Assange. There are leaks every single day in the United States, and we read about them on the front page of the *Washington Post* and the *New York Times* and for the most part we rely on the kind of discretion and judgment of newspapers to make decisions about how to tell people what's going on that people deserve to know, while at the same time protecting the secrets that need to be protected. And that's obviously a very hard call, but it's clearly not a call the government makes correctly every time. It's clearly not a call that newspapers make correctly every time. It's not a call that leakers make correctly every time. It's not a call that anyone could make correctly all the time, but that's the call that continues to need to be made. But, why should Julian Assange and WikiLeaks care? Why should the *Guardian*? The *Guardian* might care more than WikiLeaks and Julian Assange, but not necessarily. And so I do think that the stakes are higher on all sides, but I'm not sure that it really changes the paradigm because I think that, at the end of the day, the reality is that there is always going to be secrecy,

4. *See* Steve Vladeck, *Does Espionage Porn Make Us Stronger?*, JUST SECURITY, Jan. 23, 2014, http://justsecurity.org/6049/espionage-porn-stronger/.

5. John Hudson, *The Leak that Triggered the AP Phone Probe Scandal*, FOREIGN POLICY, May 14, 2013.

there always has been secrecy and secrecy has always been useful for both good ends and bad ends and that will always be true. And it's also inevitable that legislative oversight will be minimal to ineffective, that court oversight at least thus far has been virtually nonexistent, the executive oversight or insight is not particularly satisfactory either, and so at the end of the day who are we going to rely on to keep some kind of check in place? And I think it's the worst of all possible worlds but it's the best of all possible worlds. We have no alternative but to rely on some ways on leakers to keep government honest. And it's not a great system, but I honestly don't think there is a system out there; we've tried lots of systems. George listed all the harms that [] he believed Snowden caused. We could have a debate about that, but I'm not sure that's really the focus of this panel. And if it is, Steve will direct us there, but you also have to look at the benefits. So before Snowden leaked the existence of the 215 program, 15 judges had said it was okay, the executive branch had determined it was okay, two presidents have said it's fine, go right ahead, Congress had – to the extent it was aware of it – not done anything about it, and then as soon as it gets disclosed everybody is reconsidering it. The President is rolling it back. A federal court has declared it unconstitutional, an oversight board has said it was illegal because it was a blatant violation of the statute under which it was imposed, the person who drafted that statute says it was a blatant violation of the statute he drafted, Jim Sensenbrenner, right, but that's the shift that happened. And it only happened because of that leak, it only happened because of that leak, it only happened because of that leak. So I think you can't focus only on the down side of leaks. The up side of leaks is that they keep us a democracy in which we the people have something to say in how our government is acting against us and against others.

SV: That raises a question that I'd love to put to the whole panel but to George and Ken first, which is the "public value" question, because I think one possible way of thinking about distinguishing between, for example, Snowden's disclosure of the 215 program and the *Chicago Tribune*'s disclosure that we broke the Japanese naval code, is that, whether or not one agrees with Judge Leon that the 215 program is constitutional, there are certainly reasonable disagreements about the legality of the 215 program. In contrast, I don't think there would have been reasonable disagreements in 1942 about the legality of the attempts by the U.S. Naval Intelligence Service to break Japanese naval codes. I don't think anyone would have disagreed that that was so, but then the question is who makes that call, and so David's point about the media is worth underscoring; before the proliferation of the Internet usually it was the editorial boards of major newspapers that were deciding on what to print and when. I suspect the government was not always happy with how they chose to exercise that discretion, but at least they knew there was someone making that decision. We know, for example, with regard to the TSP – the Terrorist Surveillance Program – that the *New York Times* and the *Washington Post* held that story for

upwards of a year even once they had information confirming its existence.[6] My question for George and Ken is this: is the new paradigm problem simply that whatever we might have thought about the status quo in a world where it was up to newspaper editors, now it's up to anyone with access to the Internet? And if so, does that underscore Alex and David's point about how it's technology on both sides of the coin – technology with regard to the proliferation of secrecy and technology with regard to the easier ability to disseminate?

GE: Many matters have been raised in the last ten minutes about which I would like to comment. I'll try to come back to your question, as complicated as it was. I agree that there should be public discussion, public debate about such things like the 215 program – that is, the bulk meta-data program. But Snowden was the wrong way to do it. The losses that I spoke about in my initial presentation were not the result of some whacko bureaucrat wanting to classify everything and anything. If I were able to speak more specifically about these particular documents, I think you would agree with me, yes, there is absolutely good reason that they should be classified at the highest levels. I'm also concerned about the fact that there has been no public discussion in that. I see this as a failure of our political leadership. I could point you to a recently declassified opinion by Judge Eagan of FISC – the Foreign Intelligence Surveillance Court – in which she asserts that each member of Congress knew or had the opportunity to know that Section 215 was being implemented under this court's order, and she describes the order. So she has a finding that each member of Congress knew or should have known or could have known.[7] Now that should have led to some sort of discussion. The fact that it did not is certainly not the blame of the intelligence community.

SV: Do you want to say something about technology and the discretion of editorial boards versus anyone with access to a blog?

GE: Oh, I see what you mean. By the way, I want to plug Mr. Schoenfeld's book, *Necessary Secrets*. You will get the historical background to just about everything, every historical allusion we made today in a very compellingly written piece.[8] I'm going to pass on that for the moment.

SV: Ken, let me put the question to you slightly more pointedly. Isn't there a difference between someone like Manning, who disclosed basically indiscriminately large caches of documents to WikiLeaks, maybe a handful of which could easily have satisfied some definition of public concern, but many of which arguably didn't, as compared to some of this known disclosures where folks may disagree on the means of the disclosure but not the utility of having this

6. *See* Barton Gelman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST, June 7, 2013.

7. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 13-109 (FISA Ct. Aug. 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

8. GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW (2010).

public discussion. As a prosecutor is there a different mentality looking at those two cases?

KW: This goes to the exercise of prosecutorial discretion as to whether to bring these cases, and others who worked in this field will know what I'm talking about. I mean, if you take a look at the Justice Department's record, you know people saying the sky is falling because the Justice Department has brought, whatever, half dozen cases over the last six years, but I would imagine you can go in today's newspapers and find a leak in . . . a handful of leaks of classified information in the newspapers today, all of which could be prosecuted under the Federal Espionage Act. And the fact that the Justice Department has brought so few cases over the years, I think, is important. It's important in terms of measuring the impact of leak prosecutions on free press and our democracy. And the fact that the Espionage Act is unbelievably broad and can allow the Justice Department to prosecute cases all the time, prosecute both leakers as well as the press – the press can be prosecuted for having received and published the leaked information – the fact is they are very selective about the cases that they bring. They've never prosecuted a reporter. The closest they got was the AIPAC case which . . . once again, when I talk about the recipient of a leak they prosecuted the recipient of a leak in that case, not a reporter. But someone who stood in the same position as a reporter, and that case ended up being dismissed on legal and constitutional grounds. But they have never prosecuted a reporter, and I don't think it's ever going to happen in my lifetime, at least not under the typical leak scenario. There are also very selective about the leak cases they bring, and that is because there is a very strict protocol in place. You've got to go all the way up to the Attorney General to get approval for subpoenas, to get approval to prosecute the cases, and one of the things you will get, obviously, is the intent – the motivation – of the leaker. So Robert Hanssen is a pretty obvious one. His motivation was completely venal, self-glorifying, wanted money, all of that. Nobody has any sympathy for that guy. But there are true whistle blowers who you know are releasing information because they think it indicates that there is something wrong. Sometimes they are doing that because it stokes their ego, sometimes they are doing it because people just – by nature – people like to be in the know and show they are in the know and sort of get a reporter to feed their ego by giving that person information. I don't have any sympathy for that, but there are a lot of people who have mixed motives, but some are completely pure. They just want to disclose something they think is wrong. And the Justice Department looks at that, and that is something that is on the mitigating side of the balance when you decide whether or not to prosecute somebody. But under the law, under the statute, it doesn't absolve you from liability. And two, as a practical matter, it can't. As soon as the government, says so long as you are pure of heart and you are trying to fix things up in agency XYZ then we're going to give you a pass . . . well, there goes your classification system, there goes your national security confidentiality. So they don't get a pass. But to answer what was a very simple question, yeah, that is

something that is looked at very carefully. I think you've seen that in a number of the leaks that haven't been prosecuted over the last ten years.

SV: Let me ask a variation on this question. The title of the panel is a "New Paradigm of Leaking." Is there maybe a new paradigm of leak prosecutions? And that part of what we're seeing is not just more front-page headlines about leaks but also more aggressive government efforts? Now Ken, you mentioned the steps – the administrative steps – that have to be undertaken before these cases happen, but it's objectively true, as I think Charlie Savage has reported in detail, that of the nine prosecutions of national security leaks in American history, six have been during this administration.[9] I'm not good at math, but that strikes me as a lot. So, is it maybe that we don't have a new paradigm of leaking? Or whether or not we have a new paradigm of leaking, we have a new paradigm of more aggressive prosecutions of leaking, and is that something we should be worried about or should we have faith in the internal processes Ken referred to?

AA: I think that's a great question. And I think – I'm not sure if it was you, Steve, or Dave who had recently suggested that the change is really in the ability to detect leakers – it gives the government more options in terms of who to prosecute. So I don't know if the numbers actually indicate anything. To me, one of the differences is in the rhetoric that surrounds leaking. There seems to be this mentality of treating the leaking of classified information as though it's a strict liability offense. And the problem with doing that is that you don't account for, you don't account for two things: one is you don't account for the fact that there is massive over-classification in our system. And so while leaking can sometimes cause harm that outweighs the public benefit, so too can over-classification. And there is no accountability for over-classification, even when over-classification can be every bit as corrosive to our democracy by keeping out of the public domain questions that should rightly be answered by the public. So I think that's one of the problems. And the other is that there's no explicit analysis when it comes to prosecutions of this question, of the balance of the public interest versus the damage done by the leaking. And that's, in part, because the Espionage Act does not allow for it, there isn't the ability to make the case that the public interest, in knowing this information, outweighs the harm to the public. And I think under that sort of legal regime you would see someone like Edward Snowden in the United States accepting prosecution and making his case that the leaks advance the public interest more than they harm the county. But that's not the system that we live in. We live in a system where you can quickly find yourself getting 35 years even though you might not have had the same motive as someone like Hanson. You live in a system in which prosecutors, and indeed Dr. Ellard, in comparing Snowden to a classic spy, fail

9. Charlie Savage, *For U.S. Inquiries on Leaks, a Difficult Road to Prosecution*, N.Y. TIMES, June 9, 2012; *see also* Stephen I. Vladeck, *Prosecuting Leakers Under U.S. Law*, *in* WHISTLEBLOWERS, LEAKS, AND THE MEDIA: THE FIRST AMENDMENT AND NATIONAL SECURITY 29 (Paul Rosenzweig et al., eds. 2014).

to distinguish between classic spies and those who leak in the public interest. That's not to say that those who leak in the public interest should be immune from prosecution. It just means that there should be consideration of the fact that the leak is not classic espionage. It's not leaking just to the Russians, it's not leaking just to one adversary. That's the type of leak that causes pretty clear harm, when we all know maybe the NSA doesn't want us to all know, but at least the extent of the disclosures is a matter of public record, you know, and maybe more coming from reporters. But at least so far what has come out has come out by one means only, through the reporters after they have the government make their case to them. And I think that's a better world to live in than one in which all leakers are treated one and the same because then you discourage that sort of discriminating leak.

SV: David?

DC: I think I largely agree with Ken that the prosecutors have exercised a great deal of discretion in going after leakers given the plethora of leaks that we see on a weekly basis and the fact that there've been nine prosecutions in the history of the country. I also don't think the fact that there have been more under this administration than under all prior administrations means that Barack Obama somehow is less sympathetic to a free press than Richard Nixon. That is not a plausible explanation. I think a much more plausible explanation is that technology has made it easier to actually identify leakers. It used to be very hard to do so, but now it's a lot easier. But even when the prosecution acts, I think quite responsibly, they get attacked by the press. Demand for AP call records is an example. Here's a case where you've got a completely unforgiveable leak: we have an informant or an insider in a bomb-making operation in al Qaeda in the Arabian peninsula. What possible interest is there, good is there, in leaking that? None. And it's leaked, and it's reported by the AP. And so it's investigated. And they don't go right to the press. They don't say, "Tell us who was the leaker." They interview over 500 possible leakers. They spend 8 months trying to identify the old fashioned way – who's the leaker? – without success. Then they request, by subpoena, call records for a certain number of days from the bureaus that were involved in reporting the story. That's all: call records. And within a month, the perpetrator, who also was a child pornography perpetrator, FBI agent, has pled guilty.[10] And it seems to me that was a responsible response to an irresponsible leak. And even there the press, you know, came down very hard on the administration – "you're going over the line" – and the administration responded by issuing new guidelines that give even more, pay even more respect to press freedom. So I think there's a long history of respect for press freedoms, I think it's fought for diligently and sometimes over-diligently by the press, but that's an important check, and that's, I think, part of what creates the discretion that we actually see, because we have a problem of massive criminality going on in Washington every day. We have a law that is extraordinarily

10. Charlie Savage, *Former FBI Agent to Plead Guilty in Press Leak*, N.Y. TIMES (Sept. 23, 2013).

broad and could be used against any of these individuals. And you have nine cases in the history of the United States? I think that says something about the commitment to free press values that all, that virtually every administration has held to one degree or another. And when they haven't, the press have come down hard on them, and the last thing you want to do is have the press against you, and so in that sense that part of the system works.

SV: So it seems like part of what's going on might be that there is some cultural determination of . . . I mean you used the term "responsible leak versus irresponsible leak," but that begs the question, who decides when a leak is responsible versus irresponsible? I suspect that George doesn't think the answer is Edward Snowden, but if it's not Snowden, then who is it? Me?

GE: Alex is right in distinguishing Snowden from Hanssen in that Snowden did not leak simply to one of our adversaries; the problem is that he leaked to all of them. Now, there is an established process. I know David Cole doesn't find too much solace in this. Snowden could have come to me. In fact, he would have been given some protections – to the Inspector General's office, is what I mean – and we get, I'd say on the average, a thousand complaints a year on our hotline system, and we see to those. Now David says, "Oh, what would the IG do?" He'd tell Snowden, "Hey listen, 15 federal judges have certified this program as okay." There's a couple more now since David published his article in New York Review of Books[11], but we have surprising success in resolving the complaints that are brought to us. Snowden is absolutely ignorant about the material that he was interpreting; he didn't know what he was reading, as can be seen in his assertion that NSA analysts, all NSA analysts, can tap the telephone calls of all Americans, including Obama's. Simply not true. Now, I would also have an independent obligation to assess the constitutionality of that law. Perhaps it's the case that we could have shown, we could have explained to Mr. Snowden his misperceptions, his lack of understanding of what we do. If not, I would have made the Senate and House Intelligence Committees open to him. Given the reaction, I think somewhat fame by some members of that committee, I think he would have found a welcoming audience. Whether he would be, in the end, satisfied, I don't know. But allowing people who have taken an oath to protect the Constitution, to protect these national security interests, simply to violate or break that oath to me is unacceptable.

DC: Because George makes these statements, then we have, then it goes to Ken, and then you, and then Alex, and I feel like, what's the point in me responding to George? So – just so we don't lose the thought – the law that George refers to which allows a person in, a member of the Intelligence Committee, would Snowden actually have been considered a member of the Intelligence Committee? I don't know, he's a contractor, but let's assume he was. All it gives him the right to do is to go to George and say, "You know, I

11. David Cole, *The Three Leakers and What to Do About Them*, N.Y. REVIEW OF BOOKS, Feb. 6, 2014, http://www.nybooks.com/contributors/david-cole-2/.

found some abusive authority, and I'd like to present it to" – who? – to the Intelligence Committees. Well, as George has already said, the Intelligence Committees had been told about this, right? That's why Ron Wyden asked James Clapper, "Are you connecting data on millions of Americans?" Now, why James Clapper said, "No," when he knew the answer was "Yes," is another question. But Ron Wyden knew – the Intelligence Committee knew – the problem was Ron Wyden couldn't turn around and say to the American people, "Do you know what the government is doing? They're collecting data on every phone call you make." He couldn't do that. So –

SV: He couldn't go to the floor of the Senate and be protected by the Speech and Debate Clause?

DC: I don't think so. In theory, maybe, but the whole premise of the Intelligence Committee getting access to this information is that you don't turn around and turn it over to the American people. So all the whistle-blowing – the national security whistle-blower protection law – allows you to do is tell the Intelligence Committee. It does not allow you to tell people – the party – that needed to know what was going on here, which is us, the American public. That's what Edward Snowden wanted to do. I think he was appropriate in telling the American public, and no one else had done it. George hadn't done it despite his independent constitutional reviews, the courts hadn't done it despite their independent reviews, the Executive Branch hadn't done it, Congress hadn't done it, somebody has to do it. George says it's important we have a debate about this, and yet there couldn't have been a debate without a leak. So is it a crime? Yes. It's certainly a crime to violate your oath and disclose secrets. I don't think anyone on the face of this panel, much less this room would say it's not a crime. But the question isn't whether it's a crime, it's how do you balance the costs versus the benefits in the context of those crimes, and that's what all whistle-blower situations are: that people violated a rule, but, allegedly, to a greater good. And the dispute is the extent to which, you know, where that's happened and where it hasn't.

SV: I was going to tell my favorite House Intelligence Committee anecdote. I had the pleasure of testifying before the Committee in October and I got to hear Chairman Rogers actually say on the record that, basically, he observed that no one had complained in 10 years about the 215 program and said that must mean that everything was going well. And I had the temerity to interrupt him and ask, "Who would have been complaining?" to which he responded, "Well obviously your privacy's not violated if you don't know about it." If that's the chair of the House Intelligence Committee, is it possible that there's something to David's point that the current oversight regime wasn't adequate? Not for fraud and abuse, but for situations when you have individual government employees who really do believe that programs they're involved in or programs they're privy to that are authorized at the highest levels are nevertheless unlawful?

GE: I don't know the answer to the problem, and it certainly is a problem. I revert back to Judge Eagan's opinion in which she said that every member of

Congress knew or could have known about this program. I reiterate – the way this came into the public was absolutely disastrous for our national security. I can't tell you what the proper way of doing this is, but I know the way it happened was very bad.

SV: But that's the question though, right? Because George, I took you to say earlier that we should be having a public discussion about the 215 program. And I guess that begs the question, if you agree that we should be having this discussion, and you believe, as I think you've quite eloquently explained why, Snowden wasn't the right person to catalyze that discussion, is the answer really that it should have been individual members of Congress who might have been able to find out about it, maybe, if they had gone to a SCIF? And who would have, then, not have thought that they could talk about it to anybody else? Or is there some other mechanism for having the public discussion? It sounds like you think it's an appropriate discussion to be having, just not because of Snowden.

DC: And, it never would have happened without Snowden. It just wouldn't have happened. Ron Wyden couldn't have been more concerned about it, but he, obviously, did not feel that he could disclose it. He wouldn't have asked James Clapper that question. He asked that question because he wanted James Clapper to disclose it; and James Clapper, who should have said, "I can't confirm or deny," instead chose to commit perjury and lie to the American public in order to keep it secret.[12] When you've got high-level government officials lying to the American public under oath in order to keep a program secret, presumably because they understand that once it becomes public it will become a major public controversy, then, I think you really have a serious problem. And I agree with George. Deputizing lone-wolf individuals to make their own decisions about when it's appropriate or inappropriate to disclose classified information – violate their oath – that's a bad way of solving the problem. But I haven't heard a better way.

AA: You know, if you believe that there should be whistle-blowing in our democracy, then you likely believe that the method should not be just the indiscriminate disclosure of information directly to the public. And so, you probably think that there should be an intermediate step, the availability of going to the IG, the availability of going to the intelligence committees, and ultimately, maybe going to reporters who then vet the information with the government to make determinations. So, I think that's, in terms of a mode of whistle-blowing, that's probably, you know, the ideal mode. Now, I think most people who criticize Snowden just fundamentally disagree about whether most of this information should be kept secret. And the problem with that is that

12. Aaron Blake, *Sen. Wyden: Clapper didn't give 'straight answer' on NSA programs,* WASH. POST, June 11, 2013; *see also* Letter from James R. Clapper, Dir. Nat'l Intelligence, to Sen. Dianne Feinstein, Chair of Sen. Select Comm. on Intelligence (June 21, 2013), http://fas.org/irp/news/2013/07/dni-error.pdf ("[M]y response was clearly erroneous – for which I apologize.").

there's no alternative proposed. And the problem with that is it's equally untenable. If you think Snowden shouldn't be the sole person deciding, equally untenable is that the executive should be the only branch of government deciding, and that situation results in effectively handing to the executive the keys to determine what should be secret and what shouldn't. And, that's evidenced by the fact that we treat classification as though it is the effective determiner of what should be public and what should not be when, in fact, it is really an internal document management system for the executive and not something that's meant to decide the broader democratic question of what should be public and what shouldn't be public.

SV: So, Alex is making the case for an independent special advocate in the FISA court. But, Ken, I want to give you a chance to jump in.

KW: To clarify a couple things. One, David said that the reason, and don't . . . I wasn't in government over the last few years, but that the reason why executives wouldn't want to acknowledge the existence of this program is they knew it would result in the controversy that we're going through today. I don't think that's true. I think the reason why they didn't want to disclose is because it's a national security operation – its effectiveness would be completely compromised if our adversaries knew about it. And I think that's important to remember. I get it, that people can't keep secrets in government just to avoid embarrassment, or just to avoid going through the difficulty of a controversy. I would have loved to have used the classification system to just avoid embarrassing things or screw-ups on my watch, but you can't do that, alright? And we get that. And those occasions when the government does that, shame on the government, shame on the employees who do it. But just take a look at what this program is. Let's just assume it's a program that's effective. The question is, how do you give notice to the American people about this particular program? The interesting thing here is that, you know, the legal issue is, gee, did the term "relevance" apply to all this metadata, and did that justify the collection and then review of that data? All very interesting issues. And it would have been great if the FISA court could have considered that issue, written its opinion, redacted out the specifics about the targets of this surveillance, and then put that legal opinion out for the American people to chew on. Then people wouldn't have been so surprised when this came out. And maybe that would have helped to instill confidence and receive legitimacy in the eyes of the American public and Congress. But the problem is, and I was making this point yesterday with another group, how do you do that? How? This program, the effectiveness of this program, is based on its secrecy. If our adversaries know that we have compiled all this metadata; and then, when we get telephone calls, we put it in this database; and then, we can do link analysis and find out who peoples' associates are, they're going to realize, "Ooo, I gotta be careful about using that mode of communication because the government might then find out that I, person over in, you know, Karachi, am talking to someone in Providence, Rhode Island. So I'm not going to use that phone." That's going to

undermine the effectiveness of that program. So, how do you discuss the program – the legality of it – without compromising the one thing that's going to protect its effectiveness, i.e. its existence? That doesn't apply to every government program. There are a lot of programs where you could talk about it in a sanitized way, allow more out there, and not, you know, and not compromise it. But, I think it does highlight how we should have more transparency, is great in concept, but sometimes is not terribly achievable. That being said, let me just go onto the next point, which is, we have the discussions, you hear the pushback on prosecuting leakers with, "there's too much classification in the government." No question about that, and that's for a host of reasons. It's a host of operational reasons, very human reasons. It's easier to classify, and avoid making a mistake and getting in trouble, than to try to parse through and try to decide what should be classified and what shouldn't. And, there's a whole culture of over-classification. I see my friends from the Public Interest Declassification Board over there, and that's a very important issue. But it is a distinct issue from whether you prosecute or whether you sanction leaks of damaging classified information that's going to hurt the American public. And I think that's what George has said.

DC: Okay. So, first of all, I think there's a question as to whether or not 215 is compromised, or, as George said, lost, because it's been disclosed. If that were the case, then the government wouldn't be fighting to keep it going. The government would have just given it up. But, well now, Edward Snowden has disclosed it. We can save those hundreds of millions of dollars and all the electrical problems we have with the Utah facility, because we don't need to keep any of this information anymore, because it's not useful. Well, that's not the response they have. So, has it been made somewhat less useful? Quite possibly. But, then, you have to ask yourself, well, what are the terrorists – if you're a terrorist, what do you think? You look at the U.S. law on the books, and you know that the U.S. can monitor your every movement, your every communication, your every electronic communication if you're a foreign terrorist. They can monitor it all. You look at the laws, and, even if you're here in the United States, they can do it if they have reason to believe you're an agent of a foreign power or a terrorist. You don't know what they know about you; and, so, you have to assume that your calls are being monitored, that your communications are being surveilled, etc. So, the fact that now you know that my calls are, also, being kept record of, I'm not sure that that radically changes the effectiveness of the program. That's one. Two, I'm not sure that the program has been very effective. According to the government, it stopped . . . it's led to one terrorist prosecution, and that's not even a prosecution of an actual terrorist act, but a material support case.[13] But, at the end of the day, even assuming that it

13. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT, 11 (Jan. 23, 2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

would have been more effective if it's kept secret from the American people, then you have to make the bottom line question – is it appropriate in a democracy for the government to be collecting data on every American without the American people even knowing about it? I think the answer to that has to be "no." So, you have to pay the cost in terms of effectiveness of the program in order to preserve democracy.

SV: I want to try desperately to extricate us from the 215 discussion, because I suspect that minds are made up on this panel about 215. The real question, I think, was alluded to before: There was a grand compromise that the intelligence community and Congress and the courts entered into in the 1970s, which is that the justification for having these programs in secret was going to be that there would be meaningful oversight and accountability, not transparency – to use Ken's term – but certainly checks and balances, and that that oversight and accountability would come through the FISA court and the intelligence committees. If there was reason to believe that that compromise has eroded, that the oversight committees and the FISA court are not actually playing the role that was initially intended in the 70s, what everyone thinks of individual disclosures, does that at least suggest that it's worth having a public conversation about the infrastructure of oversight? About how we might better create, better empower, people? George, like you, in your position in the NSA, inspectors general, oversight committees, FISA courts, to ensure that the reasonable opposition position is heard, is represented, and, perhaps every once in a while, prevails? That, to me, is the real question going forward, which is – forget 215, forget 702, forget Snowden – is the real conversation we should be having about the structure of secret oversight and accountability?

GE: The NSA is the most heavily regulated industry in the world. I report twice a year to the Congress, very extensive reports. I report quarterly to the president's Intelligence Oversight Board. The NSA, as an agency, has similar reporting obligations. We report to the Foreign Intelligence Surveillance Court, we are under the strict oversight of my organization, and of the Department of Justice. We are continuously monitored, audited, by the Department of Justice. There is not dearth of oversight over the NSA. I think the problem and the reason we should have a debate on the matters that you raise, is that we have lost the confidence of the American people. That is, the American people, by and large, believe that we are doing something that we are not. So, I would vote for a debate on this. I would also, though, ask as a precedent to that debate, that we explain ourselves better, and that we explain the oversight system that exists.

SV: I don't think anyone disputes the *volume* of oversight to which you and your colleagues are subjected. My question is whether, in light of what we've learned over the last eight months, reasonable people could question the *efficacy* of the oversight. And, if so – I guess the point isn't to suggest more oversight for the sake of having more oversight. The point is, if there are reasonable grounds for disagreement about the efficacy of existing oversight mechanisms, isn't that a conversation the NSA should also be involved in – figuring out how

to have more effective oversight as well, if there are large chunks of the American people who don't believe that the oversight's effective?

GE: Yes and no. I don't think there have been any real questions raised about the efficacy of the oversight. Nobody I know is asserting, for instance that the NSA intentionally violated the law. Some people are saying that the law violates the Constitution. But, we abided precisely by the contours of the law. I suspect that the crisis is, however, a broad swath of people in this room don't believe that. So, again I say, yes, let's debate oversight, but I would like to see the relevant authorities made clear to the American people what the existing level of oversight is.

SV: Ken?

KW: If I could just sort of take a quick stroke of perspective on this. Keep in mind, the 1970s, they call it "the grand bargain?"

SV: Whatever you want to call it.

KW: Some kind of bargain that was struck after the Church committee hearings were sort of – there was an exposé of a lot of really egregious abuses about the intelligence community. They've sort of brought intelligence operations kind of under the law. So, you had laws limiting what the intelligence community could do; the most important one, of course, the Foreign Intelligence Surveillance Act of 1978. The intelligence committees got set up to conduct regular oversight and have complete access and get reports to them from the intelligence community about what was going on or any major events. You, also mention[ed] the FISA court oversight; you mentioned Congressional oversight; and don't forget what George represents, which is executive branch oversight, which, I could tell you, I've been on the receiving end of executive branch oversight. Actually, people dismiss it because it's the executive branch overseeing itself, but it's real, especially when it comes from [the] inspector general, who is very independent in the way it operates. So, the idea was, you set up these three different components of oversight, and that's going to keep the intelligence community within the bounds, and not have a recurrence of what we had that got exposed in the Church committee hearings. I think the system's actually worked pretty well – I think that the problem is that it's hard to think about a workable option. The notion here, especially when it comes to congressional oversight, is that they'll have full access to everything; and they do, really, pretty much have access to everything. In terms of Snowden things, as far as I know, the intelligence committees were given access to all this. The question is, okay, what can they do about it? Obviously, if a majority of the members of Congress decide that they don't like the way the government, the executive branch and the FISA court, have interpreted the definition of "relevance" in 215 and use it to do this metadata collection, they can revise – they can write, they can pass a new law. That's a pretty big hurdle. It's that fundamental question: okay, they can only do so much, but they can do a lot, because they can make your life miserable as an executive branch official if they don't like what you're doing. But, there's also that fundamental

question – how do they take the next step and actually pass a law to reign in what they disagree with? That's the problem, I think. I think the main upshot of this whole thing is that there is a lack of public confidence in what the intelligence community's doing. Some of that is really unfair. Some of it is that the government, and this is over the last couple administrations, did not do a good enough job trying to get as much of this out to the public and to the Congress as it could and should have; but it's worth it to prepare everybody for the kind of things that are being done in the name of national security. But that debate should focus on concrete, practical things. For instance, the idea of having an advocate in the FISA court; somebody who will express the other side of the equation before the FISA judges. Steve and I have debated this, and I think it can be a good idea if it's designed the right way. It could also handicap the operations, the FISA operations, but maybe that's your next question.

AA: I think to respond to what Dr. Ellard said or to pick up on that, is that the oversight mechanisms have failed, is that every branch of government has dramatically changed course in the light of day.

KW: I'd like to hear you say exactly what the course changes have been.

AA: Yeah, sure. I think David started to do the laundry list of that earlier. But, you've seen the executive branch is, now saying that the 215 program should have been public to begin with. Director Clapper has said that; the President has said that.[14] The debate has made that stronger. Agencies within the executive branch are, now, considering how to roll back the bulk collection program – maybe to end it in its current form. The judges that have heard adversarial argument about whether the program is lawful have not split on that question,[15] which is an extraordinarily important question going forward and one, you know, that there is reasonable debate on. And Congress itself has now considered over two dozen different reform measures, many of which would significantly roll back some of the – what Congress members viewed as – the greatest excesses of NSA surveillance over the last 10 years. So, I think that's the best proof that the oversight mechanisms have failed. And, the question is, how do you fix that? And I think Dr. Ellard is absolutely correct that the fix is to regain public trust. I think that the way the NSA can regain public trust is to narrow the gap between what the public generally understands the NSA to be doing and what the NSA is actually doing. And, the biggest source of mistrust was the fact that the NSA had, in secret, answered an extraordinarily important question without any public input. And that question is, are we as a society going to accept the bulk collection of information about everyday Americans? That's an extraordinarily important question that should have been debated publicly. And had it been debated publicly, I think there wouldn't have been the

14. *See, e.g.*, Spencer Ackerman, *US intelligence chief: NSA should have been more open about data collection*, THE GUARDIAN (Feb. 18, 2014), http://www.theguardian.com/world/2014/feb/18/us-intelligence-chief-nsa-open-bulk-phone-collection.

15. *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 32 (D.D.C. 2013) ("[B]ulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.").

kind of reaction that we saw. And, so, the question is, how do you narrow that gap? One way is for the intelligence community, the intelligence agencies, unilaterally to decide that certain information in a democracy simply should be public. When FISA was enacted in 1978, for example, one could have made an argument along the same lines that Ken made a moment ago, that disclosing the existence of that law or the fact that there was surveillance constrained in a particular way, would have reduced the effectiveness of the law. That maybe FISA itself as a law should be secret; the KGB would have had less of an idea about what the NSA was doing if it didn't know the protocol for surveillance under FISA. But in democracy we reject that level of secrecy. So, I think there needs to be some recognition that, simply because something could be classified doesn't mean that it should be secret in a democracy. And, I think, bulk collection is the easiest area in which to see that. There are other ways, also, of narrowing that gap: you could do things like a public advocate. But, I think all of those solutions are geared toward getting someone outside of the executive involved in the decision of what should be public and what should not be public in a democracy. And, if you've learned anything over the last 10 years, it is that the intelligence committees alone are probably not enough to draw that line; and that the FISC, at least in non-adversarial settings, is not enough to draw that line. I have some reservations about whether a public advocate could alone do that if the proceedings are kept secret. In my mind, the solution involves having at least one of those foundational constitutional and legal questions decided in public, in public courts, not in secret courts, while keeping secret appropriate intelligence sources and methods; but, at least, allowing the public insight into the big questions, the important ones, that we all have a stake in.

DC: I want to agree again with Ken. I think that the compromise, and the internal oversight, the kind of secret oversight, did work to respond to the abuses that were disclosed by the Church committee. One of the things that you see when you look at the now-disclosed FISC opinions is that, where the NSA did screw up in kind of abusing law and violating the terms of the orders under which they were supposed to be proceedings, they were called to account for it; and judges called them to account for it. So those kinds of abuses, I think, can be caught by the sort of entirely internal oversight. But, I think what this episode has taught us is that what that can't catch, is this broader question of what would the public accept? I mean to me, that's really the question here. And, I would predict that if the President doesn't end 215, Congress will, in some significant way, cut it back. Because I don't think the public will accept this; and that message was nowhere heard. It wasn't heard in the executive branch; it wasn't heard in courts; it wasn't heard in Congress. It got nowhere. Now it's become, probably, the single most important debate about privacy that has occurred in all of our lifetimes. And, so, what that indicates is that, you're not going to fix this program by tinkering with internal security, internal oversight. I agree that we should have an independent advocate in the FISC and that that would be important, but I agree with Alex, it's not sufficient. At the end

of the day, what's critical is public scrutiny in a democracy; and that's what I think this episode has most demonstrated. Somebody said in the 1950s that what democracy requires to work is transparency from the government and privacy for the citizenry. I think that, in very significant ways, we had reversed that in the United States. Where the government demanded transparency from us, but insisted on privacy for itself. And that's just no way to run a democracy.

SV: George, do you want to weigh in before we turn to audience questions?

GE: Sure. The 215 program – the bulk metadata – is done under Section 215 of the United States law. The Patriot Act. Congress reauthorized the Patriot Act some five years or so ago, leaving 215 in it. The statute is clean in its words. Again, I share Judge Eagan's exasperation when I hear that the NSA was doing something undercover. We were doing something undercover – under cover of the law.

SV: As you can see, we've reached a consensus on the panel [*laughter*], at least about the difficulty of my question. So, now, it's your turn.

Question: My question is for Mr. Ellard. I believe you said Snowden could have come to me.

GE: He could have.

Question: And, I was looking at your web site. It says, "What to expect after submitting a hotline complaint," and it says, "We cannot provide any information regarding actions that have been taken on any allegation reported to our office."[16] So, in truth, your office could have really sat on Mr. Snowden's disclosures and not provided him with any follow-up. And, to me, it sounds like from what was pretty unwavering support for the metadata program, that your office would not have investigated the legality of that. And, I'm wondering if you could comment on if that would have been the result if he had come to you, and if your website is wrong?

GE: We would have investigated the program. We would have investigated his allegations. We do that all the time. Could you repeat that phrase?

Question: Sure, it's on the "How to submit a hotline complaint. We cannot provide information regarding actions that have been taken on any allegation reported to our office."[17]

GE: I think that the person who wrote that, and I didn't, had in mind employment actions. That is if, for example, you submit a reprisal complaint asserting that you uttered some protected words, there's fraud over there, or something like that, and, then, your supervisor took an action against you, that we would protect you from that. But, if we take action against another em-

16. *See Office of the Inspector General (OIG) Hotline*, NSA.GOV, https://www.nsa.gov/about/oig/oig_hotline.shtml. The quoted material above no longer appears on the website under the "What to Expect After Submitting a Hotline Complaint." Instead, the website, which was last modified on Apr. 1, 2014, states: "Although we try to provide complainants with information regarding the outcome of our inquiries, due to privacy concerns, we are unable to provide information regarding personnel action(s) taken, if any, as a result of a complaint."

17. *Id.*

ployee, or if the agency's HR department takes action, we can't disclose what that action is. I think that's what the person who wrote those words meant.

Question: But you would follow up with the whistle-blower to talk about what investigations your office was taking?

GE: Well, we would certainly disclose the fact of an investigation. We typically disclose to the complainant the results of the investigation.

Question: Thanks to everyone for a really, really interesting discussion. My question is, what can be done to improve Congress's oversight of intelligence programs? We have internal executive branch review that is fairly robust – reasonable minds could differ about how robust it is – but there are oversight mechanisms, including lawyers saying "no" to the FBI; lawyers saying "no" to the NSA. The FISA court itself doesn't say "no" that often, but it says "not yet, go back give us some more information, justify what you're proposing before we approve it." But, one area where I think the system is pretty clearly broken down is on the legislative front. The congressional response is to write a sternly-worded letter and just file it away in a drawer until the story later breaks, or to refuse to attend classified briefings made available about the programs. Why is it not in Congress's interest to do robust oversight in a way that it is for the FISA court and for internal executive branch organs, and what can be done to incentivize Congress to do its job?

GE: I disagree with the premise that congressional oversight now is not robust. Obviously, you've never been a witness in a closed hearing of the Senate Select Intelligence Committee and been questioned by Senator Feinstein, or any of the others – it is quite robust. For example, I received a letter, perhaps four months ago, and eight members of the Senate judiciary committee called upon me to do a complete review of Section 215 of the Patriot Act, and 702 of FISA. And, I am devoting four members of my staff, full-time, for 16 months to respond to that request. The congressional oversight of the intelligence community is robust.

SV: So there is a proposal by our mutual friend, Orin Kerr, who teaches at GW, that in the context of laws, uniquely those laws that are uniquely subject to secret oversight, that Congress should adopt a categorical rule of lenity.[18] That the way to protect against a disconnect between the government's understanding of the program and the public's understanding of the program is to prevent the government from taking advantage of ambiguities in statutes in the intelligence context. I think that's worth thinking about. I actually think there's a very big difference in that regard between 215 and 702 programs. I think there's relatively more clarity from 702 what Congress was authorizing, not with regard to technological capabilities, of course, but with regard to the actual nature of the program. But that's one structural proposal: that Congress impose upon itself drafting rules that actually make it sort of, that account for the difficulties, what

18. *See* Orin Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513 (2014).

everyone thinks of the robustness of the oversight, of having to conduct such oversight entirely in secret. It's an interesting idea worth debating, in my view.

AA: I think that'd be a really interesting idea, in part, because I think the area in which oversight is most important and most lacking is not the general business of the NSA, but the areas in which the surveillance operations seemingly outplay either the law or the latest technological development in a way that would make some sort of, you know, broader-based democratic accountability meaningful. So, I think at least for those types of decisions, decisions like bulk collection, decisions about whether, you know, at what stage the Fourth Amendment injury happens – when the NSA collects the information or when it later reviews the information – those sorts of questions should be debated more broadly both within Congress and in the public. But, even if you're not on board with public oversight of that type of question, I think you could be on board with broader congressional oversight. Right now, it's very difficult if you're not on an intelligence committee to review this information notwithstanding Judge Eagan's discussion. Very few members of Congress outside of the intelligence committees actually knew about 215, and, to the extent they did know about it, they knew about it from a letter that didn't provide any legal analysis, in part because the first legal opinion written by the FISC on 215 came in August 2013, several months after the Snowden disclosures. There wasn't a legal opinion for anyone to read for the first seven years of operation of the program, you know, another consequence of the public disclosure, and the FISC saw fit to justify the program for the first time.

Question: As was mentioned, there is a debate here whether the law comports with the Constitution. When you take your oath of office, civilian or military, to serve in the United States government, the oath is to defend the Constitution. In the case of Little against Barreme,[19] a Naval officer was told even an order from the president may not be legal if it violates the Constitution. In fact, Little was held personally, personally responsible; and he obeyed an order from the president that he thought would have been legal – the Court ruled no. So, what is your responsibility under your oath if you believe this law is the law, but the law is not constitutional. What are you supposed to do?

GE: If I thought the law was not constitutional, I would resign.

SV: I will say that's the first time, in at least my 10 years in this profession, that I've ever gotten a question about the case of the *Flying Fish*. Is resignation sufficient? Would resignation send the right signal?

DC: Resignation without any explanation would leave the program under wraps. We would know that George Ellard has gone on to some other job. We wouldn't know why George Ellard had gone on to another job. It doesn't really respond to the problem. It responds to the problem from George Ellard's

19. *See* Little v. Barreme, 6 U.S. 170 (1804).

perspective, but it doesn't respond to the problem from the perspective of the nation as a whole.

GE: I spoke a little too quickly, then. There are instances of inspectors general concluding that certain programs were illegal or unconstitutional. In each of those instances, I think those people acted nobly.

DC: Point made.

Question: My question is about proxy monitoring, either inspector generals or the HPSCI and SSCI oversight.

SV: Can you explain what proxy monitoring is?

Question: Proxy monitoring is when the inspector general is acting on behalf of the public, or the HPSCI and SSCI is acting on behalf of the public. So, there's some oversight other than by the public that the HPSCI and SSCI, and the inspectors general are acting in proxy for the public to act on their behalf. So, my question is, it seems like there is a really huge disconnect between what people in the community think the efficiency and effectiveness of the IG or the HPSCI or SSCI is, versus what the public's perception of what the oversight is. So, if there is robust oversight, what can the government do to better get that information out to the public that yes, there is robust oversight by the HPSCI, and the SSCI, and the inspectors general. Is there a way that the government could do a better job of touting the successes of the HPSCI and SSCI, and touting the success of the Whistle-Blower Protection Acts, and the IG? Normally, the public gets its information through the media. And, for ill or for good, the media has a dog in the fight if the public thinks that the Whistle Blower Protection Act and the IG and the HPSCI and SSCI are doing a valiant job that may impact their ability to get certain information. So what can the government do to go directly to the public to let the public know that the oversight is robust and that there is correct oversight, and to maybe talk about the successes more?

GE: I'm not completely prepared to answer all the many questions that have been raised today. Last year, Senators Grassley and Leahy – the chairman and ranking member of the judiciary committee – wrote me a letter saying, "Tell us, in an unclassified form, unclassified response, how many intentional violations there had been of NSA authorities in the last 10 years." I answered the letter. I told them there had been 12; described to the extent I could in an unclassified document the circumstances around that. Again, I can't answer your questions, but when a demand was made on us by an appropriate authority to disclose information, we did. And that is frequent, though in a classified setting. Constantly, I'm asked by the committees to show me this report, that report. I send down to them, semi-annually I believe, perhaps quarterly, a catalog of our oversight efforts, typically in the form of written reports. And, I frequently get responses from them, "Show us this," or, "Come down and tell us about that." I think your question, though, goes to the public. The public has a right to know this.

Question: Can the government do a better job touting the successes of oversight?

GE: Yes. I'm not prepared right at this moment to make suggestions as to how that can be done.

AA: I think one of the lessons we need to take from this Snowden disclosure is that the fact of oversight has not been enough for the public. That the fact that the NSA is complying with laws that have been secretly interpreted in secret legal opinions generally pretty well, with the exception of handfuls of thousands of violations year-to-year, is not enough. That there are certain questions that the public wants answered in a different manner rather than through secret legal interpretations that are kept from the public. That form of oversight, I think, isn't one that we've heard much of an alternative for, much of a suggestion for how it occurs other than through someone like Edward Snowden. And I don't think anyone on the ACLU side of the debate now, and I won't lump David in with the ACLU, I don't think anyone takes lightly the fact that it's probably a precarious position to have only single individuals decide what should be secret and what shouldn't be secret in a democracy. But, it's equally untenable to have one branch of government decide or even all three in secret decide what should be secret when there are fundamental questions in a democracy that should be public. And answering that question is very, very difficult. I think whistle-blowers often serve a pressure-valve function: they release pressure in situations where there is this extraordinary gap. And so to my mind, it's much easier to talk about how the NSA could prevent that type of gap from coming into existence, so as to create the incentive for someone like Snowden to do what he did than it is to actually describe affirmatively the situations in which you would accept whistle-blowers. Because, I suspect, that most intelligence agency senior officials would say they never want whistle-blowers, they only want internal disclosures. I suspect that most members of the public would say that, in some circumstances, they would accept whistle-blowing; and that resolution is difficult for the government. The single thing they can, and should, do is reduce the incentive. And the way to do that is to reduce the gap in knowledge and fundamental understanding of what the laws permit.

KW: I think we are in agreement on this, but the reason I pushed back on Alex earlier is because one of the narratives is that this shows that oversight is broken. I don't think it necessarily does. And, calling on from what George has said, I think what this shows is the limits of oversight, especially congressional oversight. There is just a category where congressional oversight is based on a representative democracy, the idea that we represent your people. You're talking about proxy monitoring – the people elect representatives, some of whom get on the intelligence committees and, then, get access to this information, and they're to make the decisions on behalf of the people about these secret programs. And, when you're talking about a legal issue of this magnitude being vested in the hands of a subset of Congress without a public debate for very good classification reasons, it raises the issue. So, I think we see that this is the example of a broken system. I think it's just an example of the inherent limits of a system

where you need secrecy, but you're expecting Congress to uphold the responsibility, that in some ways, can't really be fully accomplished.

DC: And, I agree with that. And that's why I opened my remarks by saying that in some ways leakers are a terrible answer to the problem, but they're the only answer we have to the problem. If Edward Snowden hadn't raised this issue, it would not be on the table, and the United States and the world at large would not be having the most important debate about privacy and technology that has occurred in our lifetimes. And it's not about whether the internal oversight was sufficient or not, or whether George Ellard is doing a good enough job in his web site in explaining to American people what it is. The American people don't follow whether it's HPSCI, SSCI, or the FISC. You start talking about that and their eyes are going to glaze over. What they care about is the bottom line, which is that the government was collecting data on every phone call of every American without ever even asking them whether that was permissible.

Question: One can't help but wonder whether the term "congressional oversight" wasn't deliberately chosen for its ambiguity. So, Mr. Ellard correctly observed that an intelligence program can be destroyed by being disclosed, unlike most classified secrets, which don't necessarily destroy the system. What are the effects of Snowden's disclosure have been, as has been pointed out, to force terrorists to change their methods? Without getting into some weird conspiracy that Snowden was on a secret assignment from Clapper, won't the inefficiencies that will cost them to be unable to use cell phones have a great move? What is a patriot to do when one has the kinds of information Snowden had, and sees how the system deceives the American people and the Congress about what's going on? Is it more patriotic to not act? Where does one's duty lie, and how does one assess that?

SV: Thanks. Last question, please.

Question: We're talking a lot about congressional oversight, but Congress has oversight, and that's supposed to be the people. We elect them. We change who we vote for each time based on the decisions they have made. But if we can't evaluate the decisions they're making in terms of secrecy, how do we maintain the oversight of Congress that is supposed to be the final check in the system of checks and balances?

DC: Well, what would a patriot do? One thing Edward Snowden has said, I believe, is you had a pretty good life out there in Hawaii, getting paid quite well, living in the nation's paradise, free to hang out with whoever he wanted to, to go wherever he wanted. People say, "Oh, he's egomaniacal, monomaniacal, traitor" etc., but he was troubled enough by what he saw that he took steps that have basically led to his facing either a very long prison sentence or banishment from the country that he acted on behalf of, in his view, and living in seclusion. That's not an easy choice for anyone to make. I think we belittle that choice when we just condemn him. I don't know that he deserves lionization, but I do think it takes a kind of courage to put your life at risk for something you believe

in, and he did. And people disagree with him about that, but that's not an easy thing to do. I don't know what I would do. I imagine that I would have followed the law. I would not have disclosed. I would have tried to fight within the system. But, if I was Edward Snowden, no one would listen to me. I think what one has to do is one has to measure the costs, measure the benefits, act in a discriminating way which discloses only that which is necessary to disclose without disclosing things that are unnecessary and put people's lives at risk; pursue alternatives if they exist. Here, I don't think realistic alternatives really exist when the crime was not that someone was stealing money from the NSA coffers, but that the American people were kept out of this debate entirely; and the world at large kept out of the debate. When that was the crime, there wasn't really any alternative within, and so most people would just go along, take the pay, live a comfortable life, and, you know, that would be the end of it. But he took the risk. And, he is paying for the risk right now. I don't know how it will end up, but I think in some sense we rely on people to take those risks; and the fact that there are some people who will take those risks, contributes to the checks that are necessary to ensure that secrecy is not abused.

SV: Does anyone want to tackle the "Congress" question?

GE: Well, I have to apologize to the person who asked the last question because the next to last question put me over the edge. I remember hearing something about a request for me to explain how terrorists are adapting to these revelations and asking me to comment on the NSA and the government deceiving the American people. I think I've said what I'm going to say for today. It's been a pleasure. Thank you.

SV: Thank you to our last panel for a spirited conversation.