National Security Law Journal

Excerpt from Vol. 3, Issue 2 (Spring/Summer 2015)

Cite as:

Michael B. Mukasey, Symposium Address, *Safe and Surveilled: Former U.S. Attorney General Michael B. Mukasey on the NSA, Wiretapping, and PRISM*, 3 NAT'L SEC. L.J. 196 (2015).

ISSN: 2373-8464

The *National Security Law Journal* is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, intelligence, homeland security, and national defense.

We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, or sign up for our e-mail newsletter.

SYMPOSIUM ADDRESS

SAFE AND SURVEILLED:
FORMER U.S. ATTORNEY GENERAL MICHAEL B. MUKASEY ON THE NSA, WIRETAPPING, AND PRISM

The Hon. Michael B. Mukasey*

On March 26, 2014, the National Security Law Journal *at George Mason University School of Law hosted* Safe and Surveilled, *a symposium featuring a keynote address by former U.S. Attorney General Michael Mukasey, who spoke on the NSA, wiretapping, and the data-mining program known as PRISM. Following is an edited transcript of his remarks.*

I want to thank Amy [Shepard] for having me here, and George Mason for having me here, and the *National Security Law Journal* for having me here, and Jamil [Jaffer] for that splendid introduction.[1] . . . .

I'm grateful not only for the privilege of this podium but also for the fact that you're conducting this very important symposium and debate on issues that are really vital to this country—and let's face it, if we don't get this right, nothing else really matters.

---

* Eight-first Attorney General of the United States, 2007-2009.

[1] This article is an edited transcript of remarks delivered on March 26, 2014, at the *Safe and Surveilled* symposium hosted by the *National Security Law Journal* at George Mason University School of Law in Arlington, Virginia.

Now a good deal of this debate is centered around two programs of the NSA—two statutes that are used to conduct the electronic surveillance that is among this country's main defenses, sometimes its only defense, against not only state adversaries but also against people who believe that it's their religious obligation to destroy our way of life. Because this is an audience principally of lawyers, I'm going to start with the laws themselves: Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, or FISA as it's known. Then we'll examine the sources and some of the content and the criticism of these laws and the programs that they establish. The first of the two laws that I want to talk about—laws put in place after 9/11—is Section 215 of the PATRIOT Act, which allows the FBI to apply for an order from the Foreign Intelligence Surveillance Court to require the production of tangible things. It doesn't say what kinds of tangible things; it just says tangible things, and that includes business records needed for investigation to obtain foreign intelligence information about a non-U.S. person to protect the country against international terrorism.

Using that provision, the FBI has obtained a series of essentially business records orders that are renewable at 90-day intervals, which authorized the gathering of telephone metadata. The NSA, which has the technical capacity, acts on that order. It acquires the telephone metadata in bulk, and metadata—as I'm sure many or most of you know—is simply the information that [the] telephone company has on every call that's made. It's used to generate a typical telephone bill: the calling number, the number that is called, [and] the date and duration of the call. It does not include information about the content of the call. It doesn't even include information about the identity of the caller or the recipient. What the NSA does is to aggregate that data from several companies, preserving it in one place, so that it is not discarded in the normal course of business as the telephone companies sometimes do, and so it could be readily accessed.

The order, which has been approved and reapproved more than thirty-five times by at least fourteen different federal judges on the FISA court since 2006, does not allow random searching of the database, and that program has been found many times to be entirely

consistent with the Constitution and entirely lawful. When the system was in fact generating an algorithm that caused some of the few searches that were made to go beyond what was permissible, that excess was pointed out to the FISA court by the government, and the judge that heard the case and who criticized the NSA in that instance nonetheless reauthorized the program. The metadata, which after all is lawfully in the hands of the telephone companies, is not information I would suggest that is even arguably protected by the Fourth Amendment as it is actually drafted—as opposed to the Fourth Amendment as it might exist in the minds of some folks on the left and on the right.

The Fourth Amendment as drafted by the folks who did the drafting back in the day protects the rights of the people, and that means the people of this country—not people of the world over—to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. The concept that is embodied here is simply the concept of a trespass. So what is protected is their persons, and their bodies, and what they are carrying on their bodies. We still have those, of course.

What is protected against is not only a knock on the door by the constabulary, but also thermal imaging of what goes on inside your house, conducted even from several blocks away; [your] papers, which are reasonably read to include electronic storage devices like thumb drives; and effects, which is simply your stuff. It does not include the business records of a third party like a telephone company that simply keeps track of when and how long you use their equipment. Now, that's not to say that the Fourth Amendment sets the limit on what privacy protection Congress may enact if it chooses to do so, nor does it set the limit on the debate over what we want or need in the way of privacy protection. That's why you're here, and that's why you're conducting this symposium; but that is the limit of what the Fourth Amendment protects.

So, what's the information useful for? If the government gets access to a suspicious number—say, a foreign terrorist cell or a safe house—it can then run that number against the database of U.S. numbers to determine whether that number has either called or been

called by a number in the United States, [and] then examine what numbers inside and outside the United States the number that was either called or made the call has been calling. Now, obviously, if there's been contact with a suspicious number overseas and a number in the United States, further investigation can be conducted. If facts are gathered that establish probable cause to believe that a crime has been or is being committed, then a warrant can be obtained to listen in on conversations on that U.S. number, but there's no listening in unless and until a warrant is issued in the same way that warrants are issued in criminal cases and by the same standard.

The database of numbers is segregated and is not accessed for any purpose beyond the specific counterterrorism program. It's accessible only by about twenty-some odd people, counting supervisors, and the government is required to follow procedures that are overseen by the FISA court to minimize any unnecessary dissemination of U.S. numbers that are generated as a result of queries to the database. As you can imagine, that can be and indeed has been a valuable tool for protecting us from foreign-based terrorists or from domestic terrorists with foreign connections, and for detecting networks of people in this country who have ties to foreign terrorists. It's virtually the only way that the government can look outward from the United States to see what's coming in from overseas, unless we rely on good fortune in discovering what's coming overseas with the cooperation of our foreign partners. At a minimum, it could tell us that a foreign group we are looking at has not contacted anyone in the United States. We don't have to waste valuable resources or alarm people unnecessarily.

Now, there's been a good deal [of] debate on whether the Section 215 program has or hasn't resulted in the breaking of terrorist plots. Let's demystify that. If what we're talking about is whether the 215 program has scored the jump shot at the buzzer that won the game, the answer is no. On the other hand, for those of you who follow basketball, there's a lot of point-scoring that goes on before the jump shot at the buzzer that wins the game, and in that regard, it has been enormously valuable. Intelligence is gathered step by step and item by item, so it is not only the jump shot at the buzzer

that counts. In addition to being subject to court approval, the valuable Section 215 metadata program is overseen by the executive branch and by Congress, specifically the foreign intelligence and judiciary committees of both houses. When Section 215 was reauthorized in 2011, the administration briefed Members of Congress, and members of those committees, on the details of the program and provided briefing documents which were asked to be made available to all Members of Congress. Those documents included the specific disclosure that under the program, NSA acquires the call detail metadata for—this is right out of the document that was given to those committees and made available to all Members of Congress—"substantially all of the telephone calls handled by the companies [meaning the providers], including both calls made between the United States and a foreign country and calls made entirely within the United States." The committees provided briefings on those details to all those interested Members of Congress. In other words, any Member of Congress who was there in 2011 either got briefed on this, particularly if that person was a Member of either the intelligence committee or one of the judiciary committees, or had the chance to get briefed on it. They all had a chance to be briefed on it following the Snowden leaks. So if you hear that some Congressman who was actually there in 2011 has expressed surprise at this program that was reauthorized at that time, you should have the same reaction that you had if you saw the movie Casablanca when Louie the Prefect says he is "shocked, shocked" to see there is gambling going on at Rick's just before his winnings are handed to him in an envelope. They are "shocked, shocked" in exactly the same way. And yet as we sit here, more accurately as I stand here, and you sit here, the President and his administration has called for legislation that would end the gathering of this information gathered by the NSA and replace it with a system whereby the telephone companies would keep this information for no legislatively required period of time. The only period of time that they are required to keep it is under FCC regulation, and that's for eighteen months, and that of course is changeable at a moment's notice. And when the NSA wanted to run a number, it would first go to court for a judge to review the finding that that number is suspicious, and then go around to each of the providers and get each of them to search its database of numbers, rather than having all of the numbers in one

place. We can't rely on private companies to keep this information for longer then they have to, and in fact, if the FCC gets rid of its regulation that [they] have to keep it for eighteen months, it is not hard to envision a carrier saying, "Use our service, we clean house every day."

Also being presented is another proposal from people who claim to want to protect the Section 215 program that works essentially the same way. Now, I'm not going to get into the details that distinguish one legislative proposal from another, because the point that I'm trying to make is a good deal broader. The sponsors from both the administration proposal and the alternative are urging the adoption of their proposals in part because it makes it more difficult for the NSA to gather information. That is they are competing [in] who can put more obstacles in the way of the NSA, all the while claiming that none of these roadblocks makes us any less safe. But, of course, they make it more cumbersome for the NSA to gather information about people who mean us harm, and to process that information, and all of this is being done even though there is no one who has pointed to any actual misuse of this information. Rather, what we're being protected against is the possibility that somebody could misuse it. The same logic would suggest that we should disarm the police because one of them might run amok with his gun and start shooting civilians.

The other program that's been the subject of debate is administered under Section 702 of the Foreign Intelligence Surveillance Act (FISA). That program allows the Attorney General and the Director of National Intelligence to authorize jointly, for up to a year, surveillance that's targeted at foreign persons reasonably believed to be located outside this country, provided that the FISA court approves the targeting procedures under which the surveillance occurs and the minimization procedures that govern the use of the information once it's gathered. Under this program, NSA can operate within the United States to gather the content of telephone calls and Internet traffic of people outside the United States.

How's that possible? Well, it's possible because the Internet and telephone messages that flow overseas pass through servers in

the United States, so though telephone conversation or an exchange of e-mail may be between parties located entirely outside this country, the NSA can monitor cables passing through the United States to get that information. The NSA generates specific identifiers that may include, for example, telephone numbers or e-mail addresses of foreign persons outside this country, and then use[s] those identifiers to pick out communications that it is entitled to get from the general flow. The surveillance by law may not target anyone of any nationality known to be in this country or intentionally target a U.S. person anywhere in the world. In other words, they can't do reverse targeting on U.S. persons by listening in on foreign conversations. In order to get the content of communications involving anyone in the United States or any U.S. person located anywhere in the world, it's necessary to get a warrant supported by a showing of probable cause, just as one would in an ordinary criminal case.

Now, if these programs are as apparently lawful and limited as I've described, what's so controversial about them? Well, a good deal of the controversy seems rooted in the fact that until they were disclosed—mainly but not exclusively by Edward Snowden—they were secret and necessarily had to be in order to be effective. Obviously, if people know you are interested in—people that you are interested in detecting are aware of how it is that you can detect them, they can try to take steps to avoid detection. However, because of the secrecy when they were ultimately disclosed, the message was delivered by someone with a clear desire not simply to disclose what he considered to be improper conduct—but as I think I can show as obvious—was someone who wanted to injure this country. Therefore, the disclosure was accompanied by all sorts of claims of impropriety that are entirely false.

Let's take a look at who Edward Snowden is and at what he is. I suspect that there would be a good deal less support for these heroes like Snowden and others if people were aware of who they were and what they think. So, let's look for a moment at Edward Snowden, perhaps the most celebrated of these so-called whistleblowers. Actually, what I would have liked to do at this point would be to quote extensively [from] what Snowden wrote before he

knew that the world was watching and listening, but I can't do that extensively because a lot of what he wrote is the sort of thing that you don't do in mixed company or indeed in any polite company. So, let's just do a quick fly-over. Snowden's version of the story, of course, is that he became politically aware while he was working for the CIA in Geneva in 2007, when he sees surveillance going on that he thinks is improper. He considers leaking information at that time, but decides not to because Barack Obama gets elected President and he has promised hope and change. Well, there's no change, Snowden loses hope, and starts downloading information while he was employed at Dell in 2010. Then he lands a job in Hawaii with an NSA contractor—a job he sought and accepted so he could get access to even greater quantities of information. He said that he had only the purest of motives. The NSA presented what he called "an existential threat to democracy."

Sounds great, except it's not the truth. A more accurate account may be had in a splendid article by Sean Wilentz in the January issue of *The New Republic*, which I recommend to all of you.[2] Snowden is a high school dropout who developed an interest in computers, and by his own description, joined a group of what he called "alpha geeks" exploring the mysteries of sex and online gaming and sometimes firearms. At one point, he insisted—he disclosed that he had a Walther P22 that he "loved to death." In 2004, he enlists in an Army Special Forces program, but soon afterwards was granted a medical discharge when he breaks both legs in a training accident—which is something of a curiosity, because although the accident was enough to get him out of the Army, he later developed an enthusiasm for kickboxing. He says he joined the Special Forces because he felt it was his "obligation to help free people from oppression." His first employment by an intelligence agency was as a security guard at the CIA; he then becomes a security specialist, and in 2007 is posted to Geneva. Now, however Snowden felt about the administration that

[2] *See* Sean Wilentz, *Would You Feel Differently About Snowden, Greenwald, and Assange If You Knew What They Really Thought?*, NEW REPUBLIC, Jan. 19, 2014, *available at* http://www.newrepublic.com/article/116253/edward-snowden-glenn-greenwald-julian-assange-what-they-believe.

was then in power as late as January of 2009, he attacks *The New York Times* for exposing a plan to sabotage Iran's nuclear facility. He says the newspaper was like Wikileaks and deserved to go bankrupt. He urged that whoever leaked "classified shit"—his words, not mine—to the *Times* be "shot in the testicles" (that's not the word he used, but you get the picture). Economically, he supported Ron Paul's position that we should return to the gold standard, and urged that Social Security be abolished. He wrote that old people "wouldn't be [expletive deleted] helpless if you weren't sending them [expletive deleted] checks to sit on their asses and lay in hospitals all day." He made $250 contributions to Ron Paul during the 2012 primaries.

Now, although Snowden claims that he got access to highly sensitive information in the NSA by working his way up, with his considerable talents, it appears that the way he got it was by tricking one or more of his coworkers into disclosing their passwords so that he could then unleash a program that would go pick through the data to which they had access, and pick out information of the type that had been written into the program for selection. Snowden's denials here are particularly illuminating. In fact, they are Clintonian. He denies that there were legions of coworkers whose passwords he stole, to which, of course, leaves open the distinct possibility of which it was only a few. He says that he never stole any classified documents, which of course meant that he allowed the program to do it for him. He denies that he disclosed any secret information, claiming that he simply disclosed it to journalists and they decided what to publish and what not, an act he considers entirely reasonable and responsible. Of course, the journalist [to] whom he leaked the information was a writer for *The Guardian* and sometime-blogger named Glenn Greenwald. Now, there's not enough time here to explore his history, except to note that he, too, journeyed through support for Ron Paul and arrived to a worldview that seemed congenial to critics of this country's national security on both the far right and the far left.

What damage has been done to our national security by Snowden's disclosure? Well, the Defense Intelligence Agency has prepared a report for the House permanent subcommittee that's classified, but what is already clear is that although press reports have

focused on NSA foreign intelligence collection, much of the information that Snowden stole actually relates to current U.S. military operations, and in the words of [House Permanent Select Committee on Intelligence] Chairman Mike Rogers, is likely to have "lethal consequences for our troops in the field." According to the Ranking Member to the Committee Dutch Ruppersberger, we have already seen terrorists changing their methods because of Snowden's leaks. The operations affected ranged beyond terrorism, into cybercrime, narcotics, and human trafficking. A program in Latin America that helped rescue women in that part of the world from human trafficking rings had to be abandoned because documents relating to it were leaked and the identity of informants was compromised. Vital operations for all four of our military services have been affected. The exposures as to foreign intelligence operations are potentially devastating. They include, for example, an NSA report of self-assessment in fifty aspects of counterterrorism that reveals gaps in our knowledge about the security of Pakistani nuclear material when it's being transported; of the capabilities of China's next generation of fighter aircraft (that includes secrets that were stolen from our own F35 planes back in 2007); of what plans Russian leaders might have to deal with destabilizing events, such as large protests or terrorists incidents. The capabilities he has disclosed, thus far, include how NSA intercepts e-mails, phone calls, and radio transmissions of Taliban fighters in Pakistan; the fact that NSA is watching the security of Pakistan's nuclear weapons; that NSA is capable of measuring the loyalty of CIA recruits in Pakistan; [and] how NSA hacks into telephones in Honk Kong and the rest of China. Just last weekend, *The New York Times* carried another leak from the Snowden trove, a story that describes how NSA has tried—apparently successfully—to penetrate a Chinese manufacturer of electronic equipment, including communications equipment, [of] Huawei, so that it could monitor what purchasers of that equipment, including foreign governments, do with it. Right in the body of that story was the revelation that the *Times* had withheld certain technical details from the story at the request of the Obama administration, but nonetheless the Chinese government and Huawei are now on notice of the effort and can set about taking steps to guard against it.

You want to imagine the nature of the damage that he has done? Think of someone disclosing the acoustic signature of a nuclear submarine. That's among the most closely guarded of secrets that we have, because if it is disclosed, it makes that submarine—an investment of literally billions of dollars—useless. That is the nature of what he has done to a lot our intelligence capabilities.

It is, of course, no accident that Snowden has wound up in Russia, whose geopolitical goals are consistent with weakening U.S. intelligence. Russia itself is technologically and economically and militarily a basket case, but undermining the capabilities of the United States can't help [but even] the playing field. The distortion in allocating resources is another byproduct of these disclosures. As you can imagine, if a single disclosure is made, all possible sources of damage have to be considered and mitigated to the extent possible. If means and methods are disclosed, adjustments have to be made. If human assets are disclosed, steps have to be taken to get them and others with whom they may have a relationship to safety. Two disclosures complicate the problem still further. When you have millions of documents with varied disclosures, the problem of building a protective wall around what can be salvaged in each case is one that could absorb virtually the entire resources of even the best-resourced agency. And, of course, resources devoted to damage control are not then available for the active protection of our national security. But that's just the damage within our own intelligence community.

Relationships between the United States and Europe, between European nations themselves, are undermined because confidence is undermined—and I'm not speaking of the Angela Merkel cellphone problem. In fact, for years it had been an open secret in the intelligence community [that] Angela Merkel used a conventional cell phone that could be overheard, and we were by no means the only country that overheard it. The French were quite active in that regard. Besides, even if we were the only country, if you're dealing with a country like Germany that's been champing at the bit trying to avoid sanctions on Iran for years, you would certainly want to know what the leaders of that country is saying in her less-guarded moments.

Rather, what I'm talking about is simply how seriously we can be taken by even our friends. If we can't keep secrets secure from somebody like Snowden, how willing do you think foreign intelligence agencies will be to share information with us? Because the United States is a leader in the gathering of intelligence, the result is to paralyze western intelligence capabilities and our self-defense. Snowden and his public handlers . . . have sold the public in general, and some conservatives in particular, on the idea that what they have disclosed is that the United States Government is secretly spying on all of its citizens, on their communications, and indeed on all aspects of their lives—of any electronic interaction, whether through e-mail, banking, telephone calls, card transactions, you name it. They portray Snowden as romantic and idealistic rather than self-absorbed and traitorous—as someone who more closely resembles Robin Hood or Paul Revere than Alger Hiss or Benedict Arnold. And the popular press, which has an ongoing interest in being able to continue to get stories from the Snowden trough, has gone along with the message in the way it reports information, which guarantees continued access.

What this has produced is kind of an odd coalition of the extreme left, which suspects and opposes any intelligence-gathering programs [as] an actual or potential infringement of civil liberties, and the libertarian right, which suspects any branch of government and delights in conjuring up images of Big Brother so that the narrative of a spying and intrusive government comes very natural to them. As a result, we saw in the last Congress that almost half of the House of Representatives voted to defund the programs that I described, led by a coalition of libertarian Republicans and left-wing Democrats.

Of course, this isn't the first time in our history that we've seen our intelligence agencies under attack, although this is the first time that I think it's happened on this scale. Jack Goldsmith, in an excellent book called *The Terror Presidency*, published back in 2007, described what he called "cycles of aggression and timidity" in our

intelligence community.[3] As he describes it, political leaders—and he might just as well have mentioned opinion leaders, including academics and journalists—in his words, "pressure the community"—and that's the intelligence community—"to engage in controversial action at the edges of the law, and then fail to protect it from recriminations when things go awry."[4] This leads the community to retrench and become risk averse, which invites complaints by politicians that the community is fecklessly timid. Intelligence excesses in the 1960s led to the Church Committee hearings and reforms in the 1970s, which in turn led to complaints that the community had become too risk averse, which led to aggressive behavior under William Casey in the 1980s that resulted in the Iran-Contra and related scandals, which in turn led to another round of intelligence purges and restrictions in the 1990s that deepened the culture of risk aversion and once again led—both before and after 9/11—to complaints of excessive timidity.

And, of course, after 9/11 we all remember the public hearings, the 9/11 Commission, [and] other inquires that followed that awful day where the narratives produced were in many instances stories of missed opportunities. The subtext of these narratives—in fact, at times, the text—was that risk aversion can have grave costs. The 9/11 Commission report, for example, tells of operations against Osama Bin Laden that were contemplated but not executed; of surveillance considered but not requested; of information not shared; of so-called dots not connected.

Complaints about risk-averse national security were commonplace in the first few years following the September 11th attacks. This time around, the cycle threatens to damage not only careers of people involved in gathering intelligence—which is bad enough for the injury that it causes to talented and dedicated people we rely on to keep us safe, and the lessons that it teaches other talented and dedicated people who we should be able to rely on for

[3] JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 163 (2007).
[4] *Id.*

the same purpose—but also the institutions themselves, in which those careers are pursued: to some degree, the CIA, a civilian institution; but also the NSA, the National Security Agency, a military institution. So, if you were in the intelligence gathering business, and you had a family and a mortgage, how eager would you be in the current climate of suspicion to render an opinion based on what you actually believe to be the limit of the law if you think that that limit might change? Self-censorship is a real danger. The view that the NSA is a threat to civil liberties in this country is being exploited, whether ignorantly or cynically, by politicians ranging from the self-described progressives on the left to self-described libertarians on the right.

I would suggest to you that we should not be standing with the people who are trying to weaken the national security apparatus of this country. Rather than dealing in absurd imaginary scenarios of NSA employees spending their time listening in on their fellow citizens, we should be worrying about actual abuses—for example, those at the IRS—and be able to explain to those, to our fellow citizens, that in reality there is no such thing as "the government"; it's just a bunch of people. Some of them are dedicated and skilled and honest, and by and large, those people work at NSA and the CIA and other agencies where the one nightmare that keeps them awake is the possibility of another attack on this country. Others of whom are neither dedicated nor skilled nor honest, and a disproportionate number of those people work at the IRS. That should not be a hard message to get across, because in addition to simplicity, it has the truth going for it.

Now, I hope that I haven't painted too depressing of a picture of what it is that we face, and I want to end where I began. If I feel anything to be optimistic about, it's about people like you, and those you are going to hear from, who get together to discuss and debate these issues and seek the truth, because in a free country we can have no better protection than that.

Thank you very much.