Clarke Forum for Contemporary Issues

Dickinson College

Constitution Day Address

"National Security and the Constitution"

by

James A. Baker[1]

September 12, 2013

Thank you for that kind introduction, Jess. I greatly appreciate the opportunity to talk today about national security and the Constitution. It is a great honor for me to be here. Indeed, it should be a great honor for any American who has the opportunity to discuss the Constitution, especially in a setting like this.

Let me tell you what I want to talk about today: national security and the Constitution as it relates to the collection of intelligence information for cyber-security purposes. This is a topic that I fear has received far too little attention in the recent debates about government surveillance post-Edward Snowden. It is where the full range of issues regarding security, liberty, and privacy are present in acute fashion, and it is where the legal action will be in coming years.

I will approach that topic as someone who has practiced constitutional law in the context of national security, as opposed to being a constitutional legal scholar or historian. What I mean by that is that in my various national security roles in the Justice Department, including representing the government before the Foreign Intelligence Surveillance Court for over 10 years, I had to try to figure out what the Constitution

[1] The views expressed are those of Mr. Baker only and do not necessarily reflect those of any other person or entity.

actually means with respect to a wide range of pressing national security issues while at the same time people were telling me, "If we don't do this, people will die and you will be blamed." As someone once said of me, I used to make six potentially career ending decisions every day. Trying to understand the Constitution and the laws enacted under it meant a lot to me personally. And I always knew that it meant a lot to the American people, even if they would never know anything about most of the decisions that I was making. I knew I was making those decisions in their name, and I felt that pressure acutely.

Before diving into my topic, first I want to make a few comments at a higher level. First, it seems to me that what I'm going to discuss today is something that as best I can tell Americans have been discussing in one form or another since the before Constitution was ratified. I'm holding it as a fundamental paradox – many Americans don't really trust the government that we designed, nor to they fully trust the people we elected to hold the offices we created and exercise the power that we ourselves have delegated to them. And in that they may be right. I'll come back to this paradox – not necessarily trusting the very government we created – at the end of my remarks today.

Next, I also want to make a few high-level comments about our surveillance efforts post-9/11. As we all know, after 9/11 the United States went to war against al Qaeda and its affiliates and allies. I've heard it said that in war there are basically four ways to deal with the enemy: kill him, detain him, transfer him to someone else's custody, or release him. To decide which of those options makes the most sense, and to carry out such actions effectively, the President and the Intelligence Community need actionable intelligence information. One way to get such information is through

electronic surveillance. Our electronic surveillance efforts post-9/11 included the President's Surveillance Program (PSP) that President Bush authorized in 2001. One aspect of the PSP known as the Terrorist Surveillance Program (TSP) ended in early 2007, and was replaced first by a FISA court order and then by two acts of Congress – the Protect America Act (PAA) and later the FISA Amendment's Act (FAA). Section 702 of the FAA is the basis for the "Prism" program that Mr. Snowden allegedly disclosed. Other electronic surveillance tools have included traditional FISA orders, as well as the USA PATRIOT Act. Section 215 of the Patriot Act amended FISA's Business Records provision, which is the provision that the government used to authorize the collection of telephone calling records in bulk, again as allegedly disclosed by Mr. Snowden.

While all of this was going on, an increasingly significant cyber threat was emerging. In my remarks tonight, I'll first describe the cyber threat and the government's need to collect intelligence information to deal with that threat. Next, I'll comment on how our laws currently are inadequate to protect our security, liberty, and privacy. Finally, I'll discuss ten areas were we need to focus our legal reform efforts to try to achieve all of those objectives simultaneously, and point out some of the tough choices we will have to make.

First, let me orient us on the cyber field. When I refer to "cyber" I simply mean computers and computer networks. That very broad definition includes the Internet itself and all devices connected to it, as well as other computers and networks that are not so connected. Within that broad area, I'll focus on the collection of intelligence information to address the cyber threat. Such intelligence information is what enables and is

intertwined with other types of cyber activities, such as computer network exploitation (CNE), computer network defense (CND), and computer network attack (CNA). Importantly, most of the computers and computer networks I'm referring to are in private hands, which complicates significantly the security and privacy issues pertaining to cyber intelligence collection. Simultaneously protecting and spying on private networks effectively and legitimately presents difficult challenges.

One more comment at the outset. The cyber topic is so vast and complex that I'm worried that no one understands it fully, including myself. Most people are way too overconfident in their views it seems to me. Whenever you are listening to someone discuss it, retain a healthy sense of skepticism. That includes being skeptical about everything I'm saying, because I could easily be wrong in important ways.

Now let me discuss briefly the cyber threat. Malicious cyber actors threaten our country and damage it every day. These malicious actors include foreign nations, international terrorist groups, organized criminals, individual hackers, and others. They include foreign nationals and U.S. citizens. At every level of society – federal, state, and local government; public and private sector; civilian and military – we are simply not prepared to deal fully with this threat. As a result, key segments of our critical infrastructure – such as the power grid, the telecommunications system, the transportation system, and the financial sector – are not as well protected as they should be and they may be vulnerable to attack by hostile actors at time and in a manner of their choosing. Moreover, we are simply unable to protect effectively all of our intellectual property and financial assets from cyber theft. The same is true for much of our classified information.

The fact that I am here today talking about issues resulting from all of these leaks is only one example of something that happens frequently. Wikileaks is another.

Let me add one additional point at the outset about the cyber threat and contrast it with the terrorist threat. With terrorism, one of the problems is that you need to find and analyze terrorist communications in order to understand what they are planning in order to prevent attacks. In cyber, you need to find and analyze the communications, but in addition the communications themselves are the problem. The communications are the payload that the malicious actors are trying to deliver. And there are lots more of them – there simply are more pertinent communications. There is more of everything: more volume, more variety, and more velocity.

In my view the President currently possesses all of the authority he needs under the Constitution and laws of the United States to protect the country from a cyber attack. But in order for him to exercise that authority, he needs to know what threats he is facing and how best to direct our defensive and potentially offensive activities. In particular, the President needs intelligence information about the capabilities, activities, plans and intentions of malicious cyber actors. He needs to know what they are planning and how they plan to do it before an attack occurs in order to try to stop it, or to learn the identity and methodology of a successful attacker in order to retaliate and prevent further attacks. And the that fact that he currently possesses adequate authority to defend the Nation from attack does not mean that our laws cannot be improved to provide a clearer basis for the President to collect the intelligence he needs to protect the country from such a cyber attack. I'll discuss some of those improvements in a few minutes.

I'll pause for just a moment to clarify what I mean here about the word "attack." What I mean is a cyber incident that would be the equivalent, if conducted by traditional kinetic means, of an armed attack on the United States that would trigger the President's war powers under the Constitution and our right to self-defense under international law. There are reasons a true "attack" as I've described may never actually occur, and cyber-deterrence probably does exist to some important degree, so we need to act prudently here rather than hysterically. But even if an attack never occurs, cyber thieves are looting our Nation every day and compromising systems that could pave the way for an attack. We have to address those issues.

Let me go a little bit deeper into some of the types of intelligence information that the President needs to address the cyber threat. In order to detect malicious activity, one thing he needs to know is what is normal activity. He needs a baseline. In other words, for any particular network or device connected to a network, how does it operate normally? What communications does it normally process, and how does it do so? This is important in order to understand normal network behavior and attempt to detect anomalies. So next he needs to be able to detect abnormal behavior, such as malware. Malware is just malicious software or code. In other words, he needs to understand what malware looks like, and then he needs find it. One way to find malware is to scan all traffic on a network or device to determine what is malware and what is "benign-ware." This is what virus-scanning products do for example.

In addition, he needs figure out the origin of the malware. So, he needs some capability to look deep into the network, or across the Internet, to understand where in the world this stuff is coming from. And he'll also need to be able to do that by looking back

in history as it were, so he'll need access to some amount of stored data about what happened in the network in the past. Further, it's important to understand that often the malware that is sent successfully to a target device merely opens a pathway for the malicious actor to do other things with respect to that device, such as take complete command of the device, destroy it, use it to compromise other devices, and/or steal data from the device as surreptitiously as possible. So, the President will want to be able to detect and understand the command signals that a malicious actor sends to the victim device and to detect and understand the data that the malicious actor is stealing from the device and where it is going.

To do everything that I've described, the President will need metadata about cyber-activities. Metadata is just data about other data. In the cyber context, metadata includes information about how communications are routed around the Internet, such as the Internet Protocol or IP address reflecting the origin or destination of a communication. In addition to metadata, the President will also need access to the content of communications; that is, he'll need to understand the substance, purport or meaning of the communications themselves, in addition to information about the existence of the communications and the identities of the parties to the communications. Among other things, this is because he'll want to understand what the malware is doing or is intended to do. The "meaning" of the malware is content. I note that not everyone agrees with me on that point, but I think it is correct.

If you haven't figured it out by now, in order to provide the President with such a comprehensive picture of the cyber landscape the Intelligence Community or some other element of the Executive Branch, such as the Department of Homeland Security (DHS),

will want access to, and the ability to store for later examination, a huge amount of data. And that data will need to pertain not only to individual devices on a network, such as someone's smartphone, iPad, or desktop computer, but also to the myriad of devices and networks that control and operate our critical infrastructure, such as our power grid and transportation system. Moreover, in order to do everything that I have described, the President would need access to a considerable amount of data pertaining to the Internet itself, or, as some have argued, all of the data on the Internet. Let me repeat that: there are arguments that in order to defend ourselves, the government needs to be able to monitor all Internet communications. All of them. Is this possible, even if it is necessary? Maybe. The key limiting factors are money and access. And you would need lots of both.

Before moving on, it's worth noting that we're responsible in large measure for this predicament. All of the data collection that I have described might be necessary because the Internet itself is fundamentally and inherently flawed from a security perspective. I think many of us now understand that, but it bears repeating. The cyber-intelligence collection problems that I've discussed exist because as a Nation we've tolerated the production, deployment, and operation of flawed devices and networks that process and transmit our most important information and operate our most vital national systems that we ourselves have connected to this unsecure system. This is a problem of our own making.

To make matters worse, all of the cyber-intelligence collection activities I've discussed will, if successful (a big "if") merely enhance our cyber security. They are not guaranteed to make our networks and data fully secure. I'm unaware of any proposal,

procedure or technique that will solve all of our cyber-security problems. The best you can hope for right now is defense in depth using multiple layers of different types of solutions to mitigate to some degree our cyber security problems. In part this is due to the inherent flaws in our systems that I mentioned a moment ago, but it is also the result of the ever-changing techniques and activities of malicious cyber actors and the ever-present insider threat. As a result, it may make sense for us to focus as much on mitigating the effects of a successful attack as on trying to prevent one. Put differently, we should buy some flashlights and prepare for civil disorder in case the lights go out. But sensible post-cyber attack mitigation is a big topic that I can't cover today.

Returning to my main point: As you can tell from what I've said, all of the issues that people have been talking about recently in connection with Mr. Snowden and NSA regarding the nature and scope of national security surveillance are present even more acutely in the cyber realm. However, in my view the complex patchwork of statutes and rules that exists currently and that impacts intelligence collection for cyber purposes is simply not up to the task of protecting both our security and our privacy in the cyber area in a thorough, thoughtful, and comprehensive manner. Our surveillance and privacy laws need an overhaul. For example, it is often still too difficult to figure out what is lawful and what is not. This negatively impacts both intelligence collection and privacy protection. Out of confusion, lawyers can say no when they should say yes, and yes when they should say no. There are many legislative proposals out there to address some aspects of this, although everyone seems to acknowledge that none of them are perfect. But that should not prevent us from acting. Why should we wait for the malicious cyber actors to force our hand and enact sweeping reforms following a major crisis?

Addressing section 702 of the FISA Amendments Act (FAA) and section 215 of the USA PATRIOT Act, which have been the focus of recent attention, is only part of the task. You'll also need to address, to name a few, the Wiretap Act, the Pen Register Statute, the Electronic Communications Privacy Act (ECPA), FISA (including its pen register provisions and the FAA), the Communications Act of 1934, and laws governing the issuance of grand jury and administrative subpoenas. And if you really want to deal with the problem, you'll also need to address somehow analogous state and foreign laws because those impact the conduct of private companies in whose hands most of the relevant cyber information resides.

I'll turn now to ten issues that any legal reform effort will need to address. To be sure, these cover just some of the issues we need to confront to enable the President to collect the intelligence he needs to defend the Nation from cyber attack and other malicious cyber activities while at the same time putting in place real, meaningful privacy protections, oversight mechanisms, and transparency requirements that will give the American people more confidence in what he is doing in secret.

- **(1) Authority**. First, the law should provide a clear basis of authority for the full scope of the President's cyber intelligence collection activities. It should specifically authorize him to collect such intelligence, including both content and metadata. It should be clear to everyone in plain English how much authority the President has in this area. For example, if we want the President to conduct surveillance of the entire Internet, then the law should clearly say so. If we want him to do something less, then we should say so and then collectively face the consequences of our decision if something bad happens down the road.

- **(2) Limitations**. So, the law should also provide clear and constitutionally permissible limits on such authority. Such limitations might relate to the technical nature of the surveillance itself, or to the purposes for which he can conduct such surveillance and the uses he can make of such information once collected. For example, if we allow him to conduct broad-based surveillance of the Internet, for many reasons it would make sense (or be legally necessary) to clearly and strictly limit such surveillance to cyber security purposes. In addition, we'll also need to address the difficult question of whether he could use information that he collects for law enforcement purposes and, if so, under what conditions.
- **(3) Approvals**. The law should designate clearly who can approve such surveillance and on what basis. The FISA Amendments Act (FAA), for example, has a complex approval scheme that involves the Attorney General, the Director of National Intelligence, and the FISA Court. I'm not sure that is the model we should use, but the point is we need to come up with a sound arrangement for having the proper authorities approve cyber surveillance. We also need to make clear what standards the approving authorities need to apply before authorizing such surveillance and what level of proof is required. For a traditional full-content warrant probable cause is required. For metadata, it is often relevance to an authorized investigation, or sometimes specific and articulable facts giving reason to believe. The FAA has yet a different standard.
- **(4) Geography and identity**. The Internet is a physical thing. That means that all of its component parts exist somewhere in the world that can be discerned and

all of the data on it is present in one geographic location or another at any particular moment in time. Simultaneously, however, it can be difficult in real-time to determine quickly and accurately the geographic origin and intended destination of communications, and much relevant information about what is going on with respect to the Internet may not represent communications at all, at least as we traditionally think about them. And it can be difficult or impossible to determine quickly and accurately the identities of the communicants much less their citizenship or immigration status.

Our laws and policies have traditionally sought to enhance privacy protections for: (a) United States persons – meaning U.S. citizens, corporations, and permanent resident aliens; (b) all people in the United States; (c) purely domestic communications; and (d) communications with one end in the United States. However, all of that presupposes that you can tell who and where someone is. Now that can be much harder to figure out. Thus, in order to protect us from cyber threats and at the same time protect our privacy, we need to think about whether it is time to abandon our traditional focus on geography and citizenship and look to other mechanisms that protect privacy without regard to a person's status or location. One way to do so would be to simply treat all communications as if they are to, from, or about U.S. persons, and assess in a sober fashion exactly what level of privacy protection those communications require under the Constitution when collected for cyber security purposes.

- **(5) Minimization**. One of the key ways to protect privacy and ensure that surveillance activities comport with the reasonableness requirement of the Fourth

Amendment to the Constitution is to implement effective minimization procedures. This means we have to regulate the acquisition, retention, and dissemination of information that is collected. There are already pretty robust rules in place about how to do this when it comes to U.S. person communications. As I mentioned, however, the problem in the cyber area is that it can be difficult to ascertain when a communication pertains to a U.S. person, and domestic communications pose a threat as much as international communications. The law in this area needs to be updated. I don't have the answer for you here today, but related to the geography/identity problem, one possibility is to just abandon the U.S. person and foreign vs. domestic communications distinctions and focus instead on minimizing access to collected communications and metadata and the intelligence information generated from such collection, as well as the purposes for which such information can be used.

Critically, we should address the retention of collected information. That is, we need to determine how long the government can retain such information and then require destruction of such information at the end of that period. Information cannot be misused if it does not exist. A requirement that the government destroy non-pertinent communications on a date certain (say, one to two years after collection if the information is not found to be pertinent in that time period) represents one of the most important privacy protections that we can put into place.

- **(6) Information sharing with the private sector**. As I have noted, most of the Internet's infrastructure belongs to the private sector. As a result, the private

sector has access to most of the data but under present law cannot share that information with the government or can do so only under certain circumstances. But current law does not provide enough clear guidance to the government and the private sector about what can and cannot be shared, and does not preempt fully the web of state laws that further complicate any thorough analysis of what can and cannot be shared. I'm worried about whether the right information is being shared with appropriate privacy protections in place. Thus, we need to clarify what the private sector can share with the government and under what circumstances, and then provide a clear statement of immunity to limit the legal liability that such providers could face for sharing such information. All of this could be addressed by dealing with the authority and limitations issues that I mentioned a few minutes ago. Moreover, we need to address the pesky issues that arise sometimes with respect to the government sharing classified intelligence information about cyber threats with the private sector. While this is mainly a risk assessment issue, providing a clear legal foundation for such sharing could provide helpful guidance.

- **(7) Oversight**. Who should conduct oversight of all of this? Can such overseers really know what is going on and take meaningful action to address abuses? In my view, this is first and foremost a job for the Executive Branch. The President needs to put into place appropriate management mechanisms to make sure that the Executive Branch is following the law. That is one of the President's most solemn duties under the Constitution – to Take Care that the laws are faithfully executed. And then he needs to hold people accountable for following the rules.

I've written elsewhere about the challenges of conducting oversight of the Intelligence Community and I won't repeat that here. But in addition to proper management controls, we need to have one or more independent, competent, and well-funded auditors outside the management chain of command who are empowered to have access to all agency information to find out what is going on. Some Inspectors General can conduct such oversight, such as the Justice Department's IG. Others, such as NSA's IG, currently lack the institutional independence and resources to do this as robustly as will be needed if we create a structure to authorize broad cyber intelligence surveillance.

- **(8) The Role of Congress**. It is the job of Congress to authorize and fund the activities of the Executive Branch and to conduct meaningful oversight of those activities. The American people need to hold members of Congress accountable for doing so effectively. However, Congress itself is not funded, staffed or organized well enough to do this as effectively as it needs to. The Executive Branch intelligence and military activities it has authorized and funded are so vast that we need to be realistic about what we can expect from Congress. That said, Congress needs to become much more aggressive in demanding answers from the Executive Branch on what it is doing and in holding Executive Branch officials accountable. Fewer committees of jurisdiction over cyber with Members who are real experts could address some of these weaknesses, but relying on Congress alone to conduct robust oversight would be a mistake.
- **(9) Transparency**. I have said before that Americans need to be able to trust our spies, and our spies need for us to be able to trust them. The long-term viability

of Intelligence Community operations depends upon the sustained support of the American public. It is clear to me that such trust and confidence has been shaken as a result of the recent disclosures of NSA surveillance activities and errors and the extraordinary transparency that the Executive Branch provided to Congress seems to have been insufficient to quell concerns. I expect that some intelligence professionals find the reaction of some members of the public inexplicable and painful because all three branches were involved in these activities. But it is a reality they have to face. As a result, in order to carry out its work the Intelligence Community is going to have to figure out how to provide the public – and our enemies – with more transparency about what they are doing. We will need to figure out how to function in a dangerous world with an even more transparent government. I don't pretend to have the answers to these tricky questions about transparency, but more transparency is required.

- **(10) The Role of the Courts.** With the FISA Amendments Act (FAA), I'm concerned that we've already reached the outer boundaries of what we can reasonably expect a court to do with respect to foreign intelligence collection. The FISA Court consists of eleven judges, a half a dozen legal counsels, and a few staff. It cannot possibly conduct intensive oversight of every aspect of multi-billion dollar intelligence collection programs implemented by thousands of intelligence professionals. We have to be more realistic in what we expect it to do, and not push off to the Court responsibilities that others need to execute. At the end of the day, it's the President's responsibility to collect foreign intelligence in a lawful manner in order to faithfully execute his duties under the Constitution,

subject to whatever resources Congress provides for such purposes and constitutionally permissible limits it places on him.

That said, the FISA Court is a real, meaningful check on the Executive Branch. In my experience, it was no rubber stamp. It is composed of real federal judges who are independent and not beholden to the Executive Branch. It is frankly absurd to think that jurists the caliber of Royce Lamberth, Colleen Kollar-Kotelly, John Bates, and the other judges on the court were in the government's pocket or somehow colluded or collaborated with the Executive Branch. And if you obsess about the fact that the FISA Court rarely denies the government's applications, then you really don't understand how the court works or how other courts work when dealing with other types of surveillance and searches. The government almost always wins there as well. To be sure, the government could be more transparent about the FISA Court's operation and rulings, and if properly designed there could be a role for some sort of "privacy advocate." But at the end of the day the FISA Court is not a substitute for civilian control of foreign intelligence activities by elected officials who are accountable to the voters. We need all three branches focused on these issues, but the American people need to have a realistic appreciation of the limitations that each of the co-equal branches faces in addressing those issues.

* * *

So to wrap up on cyber, we face real cyber threats and the President needs to be able to collect intelligence to address those threats. Our current laws are not up to that task and need reform. Among other things, those reforms must provide clear authority

for, and constitutionally permissible limitations on, the President's cyber intelligence collection activities; clearly designate who can approve collection and on what basis; address the geography and identity problems; require proper minimization and timely destruction of non-pertinent communications, and address information sharing issues regarding the private sector; require robust oversight by all three branches of government; and provide the right amount of transparency to the American people and, by extension, our enemies.

* * *

In conclusion, I'd like to close where I started with the paradox that for many Americans we have created a government to protect our security and our liberty that we do not trust to actually do either. I'd like to quote the following words of a temporary Carlisle resident who said the following in his Farewell Address in 1796:

> This government, the offspring of our own choice, uninfluenced and unawed, adopted upon full investigation and mature deliberation, completely free in its principles, in the distribution of its powers, uniting security with energy, and containing within itself a provision for its own amendment, has a just claim to your confidence and your support. Respect for its authority, compliance with its laws, acquiescence in its measures, are duties enjoined by the fundamental maxims of true liberty. The basis of our political systems is the right of the people to make and to alter their constitutions of government. But the Constitution which at any time exists, till changed by an explicit and authentic act of the whole people, is sacredly obligatory upon all. The very idea of the power and the right of the people to establish government presupposes the duty of every individual to obey the established government.

Of course, these are the words of President George Washington. The debate today about national security and privacy to me demonstrates in part that many Americans struggle with what President Washington said, and that they are not prepared to trust the government to the extent he suggested. In the coming years, the debate about the proper balance between security and privacy as it relates to the cyber threat will once

again test our thinking about the nature of the relationship between the government and the People. I hope we are up to the task.

Thank you for your time and attention. I'd be happy to answer any questions you might have.

# # #