The NSA and Accountability in an Era of Big Data

Rajesh De*

Thank you for the introduction and the opportunity to speak today at this distinguished event.[1]

I'd also like to extend my appreciation to the Georgetown Center on National Security and the Law, as well as to the Journal of National Security Law & Policy for hosting this conference. I understand this is the first year the Journal has been co-sponsored by Georgetown Law School and the Syracuse University Institute for National Security and Counterterrorism, after many years at the McGeorge School of Law.

It is a special pleasure to be hosted by a publication that was founded by a former General Counsel for the National Security Agency, Elizabeth Rindskopf Parker. I'd also like to specifically thank Professor Carrie Cordero for graciously extending this opportunity to me and for coordinating this conference.

You have chosen a theme for today's conference that could not be more timely, significant, or challenging: "Swimming in the Ocean of Big Data: National Security Information in an Age of Unlimited Information." Looking at the agenda, it is also clear that you have a number of participants who are far more knowledgeable than I to help untangle the imperatives and complexities attendant to big data. I have admired the work of many of your panelists, and I have had the distinct pleasure of knowing several of them personally, like Dan Weitzner, with whom I worked at the White House; Alex Joel, the current Civil Liberties Protection Officer for the Office of the Director of National Intelligence (ODNI); and Beth Cook, whom NSA recently welcomed in her capacity as a member of the Privacy and Civil Liberties Oversight Board. Considering that both the ODNI as well as the Privacy and Civil Liberties Oversight Board were recommendations of the 9/11Commission, for which I served as Counsel, and were established by the Intelligence Reform and Terrorism Prevention Act, which I helped draft as a Hill staffer, it is especially rewarding to see those institutions represented by such talented individuals.

So what do I have to add to this conversation, as the relatively new General Counsel for an agency whose general approach is to stay mum whenever possible, so much so that historically its initials jokingly have been said to refer to "No Such Agency" or "Never Say Anything"? I have been General Counsel of NSA for about ten months, and I am not expert on big data like those whom you have assembled today. Moreover, much of what I have learned since joining NSA is classified, so I must take caution in how I attempt to contribute to any

---

* Rajesh De, General Counsel, National Security Agency.

[1] This article is based on remarks delivered at the Journal of National Security Law & Policy Big Data Symposium on February 27, 2013 at Georgetown University Law Center.

such discussion. Nevertheless, I believe strongly that it is important for agencies like NSA to try to be a part of the public discourse to the greatest extent possible, as ultimately its public legitimacy is strengthened by such attempts. I believe what NSA does is important for the nation; it is my role to ensure that its activities reflect its commitment to the rule of law; and I would like to help bridge a gap that has already become readily apparent in only ten months on the job: the gap between public discourse about NSA and the reality of the legal rules, oversight, and accountability that I see at work every day.

There are three pervasive false myths about NSA that I believe are belied by this reality, which I would like to address:

False Myth #1: NSA is a vacuum that indiscriminately sweeps up and stores global communications.

False Myth #2: NSA is spying on Americans at home and abroad with questionable or no legal basis.

False Myth #3: NSA operates in the shadows free from external scrutiny or any true accountability.

My concern is that these false myths may not just color public perception of NSA, but impede thoughtful discourse about the unique challenges and opportunities posed by big data in the context of national security. Before turning to these false myths, however, allow me to give you a brief overview of NSA's mission and the complex, dynamic, and evolving environment in which it operates.

***

I joined NSA as General Counsel less than a year ago, in the spring of 2012. About the time that marked my six-month anniversary at the Agency, the Agency celebrated a far more significant milestone – its 60th anniversary. NSA was established by directive of President Truman in 1952, with the aim of streamlining and consolidating the government's cryptologic assets in the aftermath of the military expansion of the Second World War, in the midst of a new conflict spurred by a surprise invasion on the Korean peninsula, and at the dawn of a decades-long Cold War under the pervasive threat of nuclear conflict. Cryptology is the business of making and breaking codes. Today, NSA employs more than 30,000 men and women located at Fort Meade, Maryland and around the world. NSA is the largest employer of mathematicians in the country; it has analysts and linguists skilled in more than 120 languages; and about half of its workforce consists of military men and women.

NSA has two primary responsibilities: signals intelligence and information assurance. The legal framework for these responsibilities includes the U.S. Constitution, Congressionally-enacted statutes, and Executive branch directives, regulations, and other guidance. NSA's signals intelligence activities are largely conducted under Executive Order 12333 ("United States Intelligence Activities") and the Foreign Intelligence Surveillance Act of 1978 ("FISA"), both of which have been amended over the years. NSA's information assurance mission is largely conducted under National Security Directive 42 ("National Policy

for the Security of National Security Telecommunications and Information Systems") and Executive Order 13587 ("Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information").

The signals intelligence responsibility is the part of the mission that most people think of with respect to NSA – i.e., collecting, analyzing, and disseminating signals intelligence for foreign intelligence and counterintelligence purposes. Signals intelligence can be derived from signals transmitting voice and internet-based communications, or signals like the electromagnetic emissions from foreign radar and weapons systems. The information assurance responsibility is to protect our communications on national security systems, namely the systems that handle classified information or are otherwise critical to military or intelligence activities. This is accomplished through activities like standard setting, communications security monitoring, and vulnerability testing.

NSA carries out these responsibilities as a member of both the Department of Defense and the Intelligence Community. This duality reflects the fact that NSA is both an agency with combat support functions and a national intelligence agency. In other words, NSA supports military operations under the direction of the Secretary of Defense and produces intelligence reporting in response to national requirements coordinated by the Director of National Intelligence.

***

NSA performs its mission in an ever more rapidly evolving operational environment, one characterized by persistent change in both the nature of our adversaries and their communications. Foreign threats are no longer limited to traditional nation state actors, or even widely-recognized terrorist groups like al Qaeda and its affiliates. Moreover, adversaries today communicate through means more operationally simple yet technically sophisticated than ever before.

As you know better than most, these changes are taking place against a backdrop of increasingly complex, dynamic, and voluminous communications data flows around the globe. Industry and academic estimates regularly chart the growth of such trends, often in metrics of such dizzying scale that they can become mind numbing: as of 2012, about 2.5 exabytes of data are created each day; more data crosses the internet every second today than was stored on the entire internet 20 years ago; global mobile traffic grew 70 percent in 2012, reaching 885 petabytes per month; and it is estimated that the number of mobile-connected devices will exceed the world's population in 2013. Scale, however, is merely one of the challenges for a signals intelligence agency like NSA-trends toward greater mobility and the increasing adoption of internet-based encryption pose additional challenges as well.

Perhaps the most alarming trend is that the digital communications infrastructure is increasingly also becoming the domain for foreign threat activity. In other words, it is no longer just a question of "collecting" or even "connecting" the dots in order to assess foreign threats amidst more and more digital noise, it is also a question of determining which of the so-called "dots" may constitute

the threat itself. As President Obama has recognized, "the cyber threat to our nation is one of the most serious economic and national security challenges we face."

Many of us read in the papers every day about cyber attacks on commercial entities. Hackers come in all shapes and sizes, from foreign government actors, to criminal syndicates, to lone individuals. But as former Secretary of Defense Leon Panetta warned a few months ago, "the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11." And as the President warned in his recent State of the Union address, we know that our enemies are "seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems."

We also have seen a disturbing trend in the evolution of the cyber threat around the world. As General Keith Alexander, the Director of NSA, describes it, the trend is one from "exploitation" to "disruption" to "destruction." In fundamental terms, the cyber threat has evolved far beyond simply stealing – the stealing of personal or proprietary information, for example-to include more disruptive activity, such as distributed denial of service attacks that may temporarily degrade websites; and more alarmingly, we now see an evolution toward truly destructive activity. Secretary Panetta, for example, recently discussed what he described as "probably the most destructive attack the private sector has seen to date" – a computer virus used to infect computers in the Saudi Arabian State Oil Company Aramco in mid-2012, which virtually destroyed 30,000 computers.

***

Within this context, big data presents opportunities and challenges for the government and the private sector. Improving our ability to gain insights from large and complex collections of data holds the promise of accelerating progress across a range of fields from health care to earth science to biomedical research. But perhaps nowhere are the challenges and opportunities of big data as stark as in the national security field, where the stakes are so high – both in terms of the threats we seek to defeat, and of the liberties we simultaneously seek to preserve. This reality is readily apparent in the evolving and dynamic cyber environment, and perhaps no more so than for an agency at the crossroads of the intelligence and the defense communities, like NSA.

Of course, NSA must necessarily operate in a manner that protects its sources and methods from public view. If a person being investigated by the FBI learns that his home phone is subject to a wiretap, common sense tells us that he will not use that telephone any longer. The same is true for NSA. If our adversaries know what NSA is doing and how it is doing it – or even what NSA is not doing and why it is not doing it – they could well find ways to evade surveillance, to obscure themselves and their activities, or to manipulate anticipated action or inaction by the U.S. government. In sum, they could more readily use the ocean of big data to their advantage.

Given the inherent limitations on discussing the details of what NSA does, I thought it might be useful to at least try to dispel certain misconceptions about NSA – particularly certain misconceptions that are relevant to the topic of big data. As one thinks about big data in any context, many of the same questions arise – many of the same questions we think about in one way or another every day at NSA: What are the characteristics of any data to be collected? How will it be acquired? For what purpose? Should data be treated differently when aggregated, or combined with other data sets? What can be done with data? Who has access to it? How and when will it be disposed? What means are there to enforce accountability with respect to the data? I hope to shed some light on how NSA considers these questions in the context of discussing three false myths that I have encountered even during my short time at the Agency.

False Myth #1: NSA is a vacuum that indiscriminately sweeps up and stores global communications.

This false myth reflects the misguided idea that NSA can and does pick up any communication, any place in the world, at any time. Put differently, this false myth presumes that NSA's discretion is the only meaningful limitation on the scope and scale of its global operations. This myth, however, ignores the reality of the legal, policy, and mission landscape within which NSA operates.

First, all intelligence activities of NSA must be properly authorized pursuant to the law and must be conducted in accordance with the law. Though this statement may sound simple, it is quite powerful. NSA only operates under positive authority – if the law does not affirmatively authorize NSA to take an action, the Agency cannot do it. Moreover, NSA must conduct authorized activities in accordance with applicable legal constraints – including those embodied in the Constitution, federal statutes, Executive Orders and other Presidential directives, as well as relevant regulations and guidance – that may limit NSA's exercise of its authorities. How NSA conducts its activities is just as important as whether it may do so, and NSA must be able to affirmatively point to the source of its authority for any activity.

As noted earlier, NSA is a foreign intelligence agency. Executive Order 12333 defines foreign intelligence as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists." This language largely mirrors that which Congress adopted in the National Security Act of 1947. FISA contains a more intricate definition of foreign intelligence information for the specific purposes of that statutory scheme, but all support the same overall conclusion – NSA's mission is neither open-ended, nor is it discretionary. NSA may only collect signals intelligence for a foreign purpose.

Second, NSA does not independently set its foreign intelligence collection requirements. NSA's collection is driven by the requirements of U.S. policy-makers and warfighters, as established through the Executive Branch and funded by Congress. For example, NSA's collection priorities are approved by the President every six months as part of the National Intelligence Priorities

Framework. In accordance with those priorities, U.S. policymakers, agencies, and the military submit their specific intelligence requirements to NSA through a formal National SIGINT Requirements Process. This process is an important policy means by which the ocean of big data is further refined for NSA's collection efforts.

Finally, from a mission perspective it would be ineffective and inefficient – indeed, it would be counterproductive – to simply collect and store as much information as possible, even absent any legal or policy constraints. This simple reality has never been more evident than in the era of big data. Every day at NSA, conversations take place about whether, even within the bounds of these legal and policy constraints, it makes sense to collect, use, or retain certain information. Simply put, it would be neither feasible nor desirable to just drain the ocean of big data into a government pool of big data.

False Myth: #2: NSA is spying on Americans at home and abroad with questionable or no legal basis.

This false myth reflects both deep philosophical distrust of the secretive NSA by some, and the reality that signals intelligence activities, unlike some other intelligence activities, inevitably implicate the privacy rights of U.S. persons. It also reflects more recent controversy over so-called "warrantless wiretapping" under the President's Terrorist Surveillance Program (TSP). Without getting into details about the TSP (the authorization for which ended in 2007, but much of which is still classified and the subject of litigation) or FISA (an intricate statutory scheme), I would like to make a few general points about our current operations to help dispel this myth.

First, without an individualized determination of probable cause by a federal judge, NSA does not target the communications of any unconsenting U.S. person anywhere in the world when there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes in the United States (note that pursuant to statute and regulation, under certain emergency scenarios the Attorney General can make an initial finding of probable cause, but if within the purview of FISA, the Foreign Intelligence Surveillance Court must subsequently make that determination). One point worth highlighting in particular is that, amidst the controversy over the recent amendments made to FISA in 2008 and reauthorized in 2012, an important change was made: targeting a U.S. person abroad now requires a probable cause finding by a federal judge, whereas previously it could be approved by the Attorney General alone under Executive Order 12333.

Second, under even one of the more controversial provisions of the recent FISA amendments, Section 702, where no individualized probable cause finding is required, express limits were enacted:

- Section 702 may only be used to target non-U.S. persons reasonably believed to be located outside the United States.

- Section 702 may not be used to intentionally target any person in the United States or a U.S. person outside the United States.
- Section 702 may not be used to conduct "reverse targeting" – i.e., targeting of a person outside the United States if the purpose is to target a particular, known person inside the United States.
- Section 702 may not be used to intentionally acquire a "wholly-domestic communication" – i.e., a communication where all communicants are inside the United States.
- Section 702 must be implemented in a manner consistent with the Fourth Amendment.

Third, to the extent that information to, from, or about U.S. persons is acquired incidentally as part of NSA's foreign intelligence mission, there are specifically-tailored and externally-approved rules in place to address the collection, handling, use, and destruction of such information consistent with the Fourth Amendment. These rules are called "minimization procedures." Although public dialogue has more commonly concerned the procedures required by statute (minimization procedures are required by FISA, which must be approved by the FISC), NSA has in fact long been required by Executive Order 12333 and Department of Defense regulation to handle U.S. person information in accordance with procedures approved by the Attorney General and consistent with the Fourth Amendment.

FISA defines minimization procedures generally as "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." Not much has been disclosed about the details of these procedures to avoid providing a roadmap to spies, terrorists, and foreign governments looking to circumvent U.S. intelligence efforts, but I would like to make a few general points here.

- The underlying presumption for minimization procedures-that information to, from, or about U.S. persons inevitably will be acquired during the course of foreign intelligence activities – has been anticipated and accepted by all three branches of our government for decades. The legislative requirement for court-approved minimization procedures dates back to 1978, and the executive branch has required Attorney General approved procedures for the handling of U.S. person information since at least the signing of Executive Order 12333 in 1981.
- Minimization procedures are multi-faceted in that they are designed to address each stage of the intelligence process – from acquisition to use to dissemination to retention of information. Such procedures should be

considered holistically, with interrelated constraints that span across the entire intelligence process. These constraints may be procedural, technological, or substantive limits on how information may be acquired, how it may be handled, who may see it, or when it must be destroyed. Significantly, FISA provides that the dissemination of information about U.S. persons is expressly prohibited unless it is necessary to understand foreign intelligence or assess its importance; is evidence of a crime; or indicates a threat of death or serious bodily harm.

- Minimization procedures are specifically tailored-in other words, there is no one-size fits all set of procedures for all data for all time. As FISA states, these procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance." Relevant to such analysis would be considerations about the intrusiveness of the surveillance techniques involved; the nature of the data acquired; the reason for the acquisition; and the likelihood of any incidental U.S. person information.

These procedures are one means by which the acquisition, retention, and dissemination of U.S. person information can be appropriately protected even in the era of big data.

False Myth #3: NSA operates in the shadows free from external scrutiny or any true accountability.

This false myth is obviously a product of the necessarily secretive nature of NSA's day-to-day operations. There is no doubt that in a democracy like ours, an important form of accountability is public transparency. However, it is absolutely essential not to assume that the legitimacy afforded by public transparency is the only way to achieve accountability, which may – in fact, must, with respect to NSA – primarily be achieved through alternate means. There is no perfect substitute for public transparency in a democracy; but when there is also no way to provide information to those whom you seek to protect without also providing it to those from whom you seek to protect them, we must largely rely on such alternate means of accountability.

It is evident to me that I am the General Counsel for one of the most highly regulated entities in the world. It is a reality that most audiences cannot appreciate given the classified nature of intelligence work. Given NSA's unique mission, however, it makes perfect sense. NSA is part of the Department of Defense as well as the Intelligence Community. This means that NSA is subject to the relevant rules and regulations for DOD as well as to those applicable to other members of the IC. More broadly, NSA is subject to a spectrum of detailed scrutiny from across all three branches of government as a matter of law, policy, and practice. First, within the executive branch alone, NSA is responsible to multiple stakeholders, including:

- internal oversight officials, including an Inspector General to whom Congress recently provided independent statutory authority under the 2010 Intelligence Authorization Act;
- the Department of Defense, which pursuant to presidential directive and statute exercises supervisory authority over NSA, to include officials such as the Assistant to the Secretary for Intelligence Oversight, the Under Secretary of Defense for Intelligence, the General Counsel, and the DOD Inspector General;
- the Office of the Director of National Intelligence, which pursuant to presidential directive and statute is responsible for coordination of the Intelligence Community, and has an oversight role with respect to certain FISA activities, to include its own General Counsel, Inspector General, and Civil Liberties Protection Officer;
- the Department of Justice, which by statute also has an oversight role with respect to certain FISA activities, and to which NSA like other intelligence agencies is obligated by statute and Executive Order 12333 to report violations of federal law;
- the White House, to include the National Security Council, the President's Intelligence Advisory Board, and the Intelligence Oversight Board, to whom NSA like other intelligence agencies is required to report "any intelligence activities . . . that they have reason to believe may be unlawful or contrary to executive order or presidential directive"; and
- independent entities such as the Privacy and Civil Liberties Oversight Board.

Second, apart from the multiple layers of accountability within the executive branch, NSA is by law accountable to the legislative branch. As a member of the Intelligence Community, NSA is required by law to keep the intelligence oversight committees of the Senate and House of Representatives "fully and currently informed" with respect to the Agency's activities. Given the unique role of NSA and the range of its activities, however, oversight is exercised as well by a host of additional committees as diverse as the armed services, judiciary, and homeland security committees of both chambers of Congress. NSA, for example, is required by statute to provide both the intelligence and judiciary committees a copy of any decision, order, or opinion of the FISC that includes "significant construction or interpretation" of any provision of FISA. NSA also keeps Congress apprised of its activities routinely via testimony at open and closed hearings; formal notifications; other written submissions; informal briefings, visits; and other means. In other words, we interact with our Congressional overseers virtually every day.

Third, NSA is directly accountable to the Foreign Intelligence Surveillance Court for those activities conducted pursuant to FISA. The Court is comprised of eleven federal district judges appointed by the Chief Justice of the U.S. Supreme Court. The FISC not only authorizes certain activities pursuant to

FISA, but it plays an active and constructive role in ensuring those activities are carried out appropriately. As I noted earlier, it is evident that the manner in which NSA operates is just as important as the authority under which it operates. The rules of the FISC, for example, reflect this commitment in that "[i]f the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law," the government must "immediately" notify the Court. This obligation is one that NSA, together with our partners at the Department of Justice, take seriously every single day.

Finally, NSA traditionally has maintained a strong culture of compliance among its workforce. Employees receive basic mandatory training on NSA's legal authorities and the procedures that ensure the protection of privacy rights. Personnel also must receive refresher training throughout their career at NSA. Follow-on training can include highly specialized legal and compliance training focused on the specific requirements of the employee's assigned mission. NSA has also proactively established a corporate Director of Compliance to help ensure that legal, technical, and operational requirements of the mission remain aligned. NSA's compliance efforts draw from best practices across industry (such as IT security and other heavily regulated industries like healthcare). NSA is actively engaging with the broader compliance community to partner, to share best practices, and to understand emerging trends.

***

Big data is transforming the world in which NSA carries out its mission, but NSA is constantly evolving in terms of the mix of technology, resources, skills, and authorities necessary to take advantage of its opportunities and meet its challenges. What remains constant is NSA's commitment to the law; to the notion that how the Agency conducts its activities is just as important as whether it is authorized to conduct them. Although much of the detail by necessity must remain secret, a great deal gets lost in the public discourse about the legal framework within which NSA conducts its mission, its requirement for specifically tailored and externally approved minimization procedures, and the robust oversight structures in place across all three branches of government. These features are as much a part of the reality in which NSA operates today as is the reality of big data.