FIRST IMPRESSIONS, OBAMA'S SPEECH

I will write far more on the President's speech and new Directive. But here are some early thoughts.

Obama used the example of Paul Revere as an example of the importance of intelligence over the life of "our country." Of course, Paul Revere is actually a better example that, if the Brits had done metadata analysis akin to what he preserved today, we would still be eating Kidney pies under British rule.

Obama made no mention, at all, of NSA's weakening encryption and hoarding zero days. None.

With the sole exception of consulting with Congress on how to resolve the Section 215 dragnet (something that will happen during next year's PATRIOT Act Reauthorization if not before) these changes are all Executive Branch self-limitations. Even the role of a FISC advocate fell by the wayside. In other words, while Obama did call for some useful changes (limiting the gag order on NSLs, adding limits on the way back door searches can be used for criminal investigations), they're all self-limitations that can't be enforced or overseen.

At one point, Obama justified our dragnet by saying we have special responsibilities as the only Superpower. Now, China is getting big enough they might object to that whole claim. More importantly, it demonstrates the degree to which a presumption of exceptionalism underlies our entire approach to spying.

See below for speech as written.

At the dawn of our Republic, a small, secret surveillance committee borne out of the "The Sons of Liberty" was established in Boston. The

group’s members included Paul Revere, and at night they would patrol the streets, reporting back any signs that the British were preparing raids against America’s early Patriots.

Throughout American history, intelligence has helped secure our country and our freedoms. In the Civil War, Union balloon reconnaissance tracked the size of Confederate armies by counting the number of camp fires. In World War II, code-breaking gave us insight into Japanese war plans, and when Patton marched across Europe, intercepted communications helped save the lives of his troops. After the war, the rise of the Iron Curtain and nuclear weapons only increased the need for sustained intelligence-gathering. And so, in the early days of the Cold War, President Truman created the National Security Agency to give us insight into the Soviet bloc, and provide our leaders with information they needed to confront aggression and avert catastrophe.

Throughout this evolution, we benefited from both our Constitution and traditions of limited government. U.S. intelligence agencies were anchored in our system of checks and balances – with oversight from elected leaders, and protections for ordinary citizens. Meanwhile, totalitarian states like East Germany offered a cautionary tale of what could happen when vast, unchecked surveillance turned citizens into informers, and persecuted people for what they said in the privacy of their own homes.

In fact even the United States proved not to be immune to the abuse of surveillance. In the 1960s, government spied on civil rights leaders and critics of the Vietnam War. Partly in response to these revelations, additional laws were established in the 1970s to ensure that our intelligence capabilities could not be misused against our citizens. In the long, twilight struggle against Communism, we had been reminded that the very liberties that we sought to preserve could not be sacrificed at the altar of national security.

If the fall of the Soviet Union left America without a competing superpower, emerging threats

from terrorist groups, and the proliferation of weapons of mass destruction placed new – and, in some ways more complicated – demands on our intelligence agencies. Globalization and the Internet made these threats more acute, as technology erased borders and empowered individuals to project great violence, as well as great good. Moreover, these new threats raised new legal and policy questions. For while few doubted the legitimacy of spying on hostile states, our framework of laws was not fully adapted to prevent terrorist attacks by individuals acting on their own, or acting in small, ideologically driven groups rather than on behalf of a foreign power.

The horror of September 11th brought these issues to the fore. Across the political spectrum, Americans recognized that we had to adapt to a world in which a bomb could be built in a basement, and our electric grid could be shut down by operators an ocean away. We were shaken by the signs we had missed leading up to the attacks – how the hijackers had made phone calls to known extremists, and travelled to suspicious places. So we demanded that our intelligence community improve its capabilities, and that law enforcement change practices to focus more on preventing attacks before they happen than prosecuting terrorists after an attack.

It is hard to overstate the transformation America's intelligence community had to go through after 9/11. Our agencies suddenly needed to do far more than the traditional mission of monitoring hostile powers and gathering information for policymakers – instead, they were asked to identify and target plotters in some of the most remote parts of the world, and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated with spies or informants.

And it is a testimony to the hard work and dedication of the men and women in our intelligence community that over the past decade, we made enormous strides in fulfilling this mission. Today, new capabilities allow

intelligence agencies to track who a terrorist is in contact with, and follow the trail of his travel or funding. New laws allow information to be collected and shared more quickly between federal agencies, and state and local law enforcement. Relationships with foreign intelligence services have expanded, and our capacity to repel cyber-attacks has been strengthened. Taken together, these efforts have prevented multiple attacks and saved innocent lives – not just here in the United States, but around the globe as well.

And yet, in our rush to respond to very real and novel threats, the risks of government overreach – the possibility that we lose some of our core liberties in pursuit of security – became more pronounced. We saw, in the immediate aftermath of 9/11, our government engaged in enhanced interrogation techniques that contradicted our values. As a Senator, I was critical of several practices, such as warrantless wiretaps. And all too often new authorities were instituted without adequate public debate.

Through a combination of action by the courts, increased congressional oversight, and adjustments by the previous Administration, some of the worst excesses that emerged after 9/11 were curbed by the time I took office. But a variety of factors have continued to complicate America's efforts to both defend our nation and uphold our civil liberties.

First, the same technological advances that allow U.S. intelligence agencies to pin-point an al Qaeda cell in Yemen or an email between two terrorists in the Sahel, also mean that many routine communications around the world are within our reach. At a time when more and more of our lives are digital, that prospect is disquieting for all of us.

Second, the combination of increased digital information and powerful supercomputers offers intelligence agencies the possibility of sifting through massive amounts of bulk data to identify patterns or pursue leads that may thwart impending threats. But the government collection and storage of such bulk data also creates a

potential for abuse.

Third, the legal safeguards that restrict surveillance against U.S. persons without a warrant do not apply to foreign persons overseas. This is not unique to America; few, if any, spy agencies around the world constrain their activities beyond their own borders. And the whole point of intelligence is to obtain information that is not publicly available. But America's capabilities are unique. And the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do.

Finally, intelligence agencies cannot function without secrecy, which makes their work less subject to public debate. Yet there is an inevitable bias not only within the intelligence community, but among all who are responsible for national security, to collect more information about the world, not less. So in the absence of institutional requirements for regular debate – and oversight that is public, as well as private – the danger of government overreach becomes more acute. This is particularly true when surveillance technology and our reliance on digital information is evolving much faster than our laws.

For all these reasons, I maintained a healthy skepticism toward our surveillance programs after I became President. I ordered that our programs be reviewed by my national security team and our lawyers, and in some cases I ordered changes in how we did business. We increased oversight and auditing, including new structures aimed at compliance. Improved rules were proposed by the government and approved by the Foreign Intelligence Surveillance Court. And we sought to keep Congress continually updated on these activities.

What I did not do is stop these programs wholesale – not only because I felt that they made us more secure; but also because nothing in that initial review, and nothing that I have learned since, indicated that our intelligence community has sought to violate the law or is

cavalier about the civil liberties of their fellow citizens.

To the contrary, in an extraordinarily difficult job, one in which actions are second-guessed, success is unreported, and failure can be catastrophic, the men and women of the intelligence community, including the NSA, consistently follow protocols designed to protect the privacy of ordinary people. They are not abusing authorities in order to listen to your private phone calls, or read your emails. When mistakes are made – which is inevitable in any large and complicated human enterprise – they correct those mistakes. Laboring in obscurity, often unable to discuss their work even with family and friends, they know that if another 9/11 or massive cyber-attack occurs, they will be asked, by Congress and the media, why they failed to connect the dots. What sustains those who work at NSA through all these pressures is the knowledge that their professionalism and dedication play a central role in the defense of our nation.

To say that our intelligence community follows the law, and is staffed by patriots, is not to suggest that I, or others in my Administration, felt complacent about the potential impact of these programs. Those of us who hold office in America have a responsibility to our Constitution, and while I was confident in the integrity of those in our intelligence community, it was clear to me in observing our intelligence operations on a regular basis that changes in our technological capabilities were raising new questions about the privacy safeguards currently in place. Moreover, after an extended review of our use of drones in the fight against terrorist networks, I believed a fresh examination of our surveillance programs was a necessary next step in our effort to get off the open ended war-footing that we have maintained since 9/11. For these reasons, I indicated in a speech at the National Defense University last May that we needed a more robust public discussion about the balance between security and liberty. What I did not know at the

time is that within weeks of my speech, an avalanche of unauthorized disclosures would spark controversies at home and abroad that have continued to this day.

Given the fact of an open investigation, I'm not going to dwell on Mr. Snowden's actions or motivations. I will say that our nation's defense depends in part on the fidelity of those entrusted with our nation's secrets. If any individual who objects to government policy can take it in their own hands to publicly disclose classified information, then we will never be able to keep our people safe, or conduct foreign policy. Moreover, the sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come.

Regardless of how we got here, though, the task before us now is greater than simply repairing the damage done to our operations; or preventing more disclosures from taking place in the future. Instead, we have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals – and our Constitution – require. We need to do so not only because it is right, but because the challenges posed by threats like terrorism, proliferation, and cyber-attacks are not going away any time soon, and for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world.

This effort will not be completed overnight, and given the pace of technological change, we shouldn't expect this to be the last time America has this debate. But I want the American people to know that the work has begun. Over the last six months, I created an outside Review Group on Intelligence and Communications Technologies to make recommendations for reform. I've consulted with the Privacy and Civil Liberties Oversight Board. I've listened to

foreign partners, privacy advocates, and industry leaders. My Administration has spent countless hours considering how to approach intelligence in this era of diffuse threats and technological revolution. And before outlining specific changes that I have ordered, let me make a few broad observations that have emerged from this process.

First, everyone who has looked at these problems, including skeptics of existing programs, recognizes that we have real enemies and threats, and that intelligence serves a vital role in confronting them. We cannot prevent terrorist attacks or cyber-threats without some capability to penetrate digital communications – whether it's to unravel a terrorist plot; to intercept malware that targets a stock exchange; to make sure air traffic control systems are not compromised; or to ensure that hackers do not empty your bank accounts.

Moreover, we cannot unilaterally disarm our intelligence agencies. There is a reason why blackberries and I-Phones are not allowed in the White House Situation Room. We know that the intelligence services of other countries – including some who feign surprise over the Snowden disclosures – are constantly probing our government and private sector networks, and accelerating programs to listen to our conversations, intercept our emails, or compromise our systems. Meanwhile, a number of countries, including some who have loudly criticized the NSA, privately acknowledge that America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities; and that they themselves have relied on the information we obtain to protect their own people.

Second, just as ardent civil libertarians recognize the need for robust intelligence capabilities, those with responsibilities for our national security readily acknowledge the potential for abuse as intelligence capabilities advance, and more and more private information

is digitized. After all, the folks at NSA and other intelligence agencies are our neighbors and our friends. They have electronic bank and medical records like everyone else. They have kids on Facebook and Instagram, and they know, more than most of us, the vulnerabilities to privacy that exist in a world where transactions are recorded; emails and text messages are stored; and even our movements can be tracked through the GPS on our phones.

Third, there was a recognition by all who participated in these reviews that the challenges to our privacy do not come from government alone. Corporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes; that's how those targeted ads pop up on your computer or smartphone. But all of us understand that the standards for government surveillance must be higher. Given the unique power of the state, it is not enough for leaders to say: trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached. Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power; it depends upon the law to constrain those in power.

I make these observations to underscore that the basic values of most Americans when it comes to questions of surveillance and privacy converge far more than the crude characterizations that have emerged over the last several months. Those who are troubled by our existing programs are not interested in a repeat of 9/11, and those who defend these programs are not dismissive of civil liberties. The challenge is getting the details right, and that's not simple. Indeed, during the course of our review, I have often reminded myself that I would not be where I am today were it not for the courage of dissidents, like Dr. King, who were spied on by their own government; as a President who looks at intelligence every morning, I also can't help but be reminded that America must be vigilant in the face of threats.

Fortunately, by focusing on facts and specifics rather than speculation and hypotheticals, this review process has given me – and hopefully the American people – some clear direction for change. And today, I can announce a series of concrete and substantial reforms that my Administration intends to adopt administratively or will seek to codify with Congress.

First, I have approved a new presidential directive for our signals intelligence activities, at home and abroad. This guidance will strengthen executive branch oversight of our intelligence activities. It will ensure that we take into account our security requirements, but also our alliances; our trade and investment relationships, including the concerns of America's companies; and our commitment to privacy and basic liberties. And we will review decisions about intelligence priorities and sensitive targets on an annual basis, so that our actions are regularly scrutinized by my senior national security team.

Second, we will reform programs and procedures in place to provide greater transparency to our surveillance activities, and fortify the safeguards that protect the privacy of U.S. persons. Since we began this review, including information being released today, we have declassified over 40 opinions and orders of the Foreign Intelligence Surveillance Court, which provides judicial review of some of our most sensitive intelligence activities – including the Section 702 program targeting foreign individuals overseas and the Section 215 telephone metadata program. Going forward, I am directing the Director of National Intelligence, in consultation with the Attorney General, to annually review – for the purpose of declassification – any future opinions of the Court with broad privacy implications, and to report to me and Congress on these efforts. To ensure that the Court hears a broader range of privacy perspectives, I am calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before

the Foreign Intelligence Surveillance Court.
Third, we will provide additional protections for activities conducted under Section 702, which allows the government to intercept the communications of foreign targets overseas who have information that's important for our national security. Specifically, I am asking the Attorney General and DNI to institute reforms that place additional restrictions on government's ability to retain, search, and use in criminal cases, communications between Americans and foreign citizens incidentally collected under Section 702.
Fourth, in investigating threats, the FBI also relies on National Security Letters, which can require companies to provide specific and limited information to the government without disclosing the orders to the subject of the investigation. These are cases in which it is important that the subject of the investigation, such as a possible terrorist or spy, isn't tipped off. But we can – and should – be more transparent in how government uses this authority. I have therefore directed the Attorney General to amend how we use National Security Letters so this secrecy will not be indefinite, and will terminate within a fixed time unless the government demonstrates a real need for further secrecy. We will also enable communications providers to make public more information than ever before about the orders they have received to provide data to the government.
This brings me to program that has generated the most controversy these past few months – the bulk collection of telephone records under Section 215. Let me repeat what I said when this story first broke – this program does not involve the content of phone calls, or the names of people making calls. Instead, it provides a record of phone numbers and the times and lengths of calls – meta-data that can be queried if and when we have a reasonable suspicion that a particular number is linked to a terrorist organization.
Why is this necessary? The program grew out of a

desire to address a gap identified after 9/11. One of the 9/11 hijackers – Khalid al-Mihdhar – made a phone call from San Diego to a known al Qaeda safe-house in Yemen. NSA saw that call, but could not see that it was coming from an individual already in the United States. The telephone metadata program under Section 215 was designed to map the communications of terrorists, so we can see who they may be in contact with as quickly as possible. This capability could also prove valuable in a crisis. For example, if a bomb goes off in one of our cities and law enforcement is racing to determine whether a network is poised to conduct additional attacks, time is of the essence. Being able to quickly review telephone connections to assess whether a network exists is critical to that effort.

In sum, the program does not involve the NSA examining the phone records of ordinary Americans. Rather, it consolidates these records into a database that the government can query if it has a specific lead – phone records that the companies already retain for business purposes. The Review Group turned up no indication that this database has been intentionally abused. And I believe it is important that the capability that this program is designed to meet is preserved.

Having said that, I believe critics are right to point out that without proper safeguards, this type of program could be used to yield more information about our private lives, and open the door to more intrusive, bulk collection programs. They also rightly point out that although the telephone bulk collection program was subject to oversight by the Foreign Intelligence Surveillance Court and has been reauthorized repeatedly by Congress, it has never been subject to vigorous public debate. For all these reasons, I believe we need a new approach. I am therefore ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk

meta-data.

This will not be simple. The Review Group recommended that our current approach be replaced by one in which the providers or a third party retain the bulk records, with the government accessing information as needed. Both of these options pose difficult problems. Relying solely on the records of multiple providers, for example, could require companies to alter their procedures in ways that raise new privacy concerns. On the other hand, any third party maintaining a single, consolidated data-base would be carrying out what is essentially a government function with more expense, more legal ambiguity, and a doubtful impact on public confidence that their privacy is being protected.

During the review process, some suggested that we may also be able to preserve the capabilities we need through a combination of existing authorities, better information sharing, and recent technological advances. But more work needs to be done to determine exactly how this system might work.

Because of the challenges involved, I've ordered that the transition away from the existing program will proceed in two steps. Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of three. And I have directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period, the database can be queried only after a judicial finding, or in a true emergency.

Next, I have instructed the intelligence community and Attorney General to use this transition period to develop options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address without the government holding this meta-data. They will report back to me with options for alternative approaches before the program comes up for reauthorization on March 28. During this period, I will consult

with the relevant committees in Congress to seek their views, and then seek congressional authorization for the new program as needed. The reforms I'm proposing today should give the American people greater confidence that their rights are being protected, even as our intelligence and law enforcement agencies maintain the tools they need to keep us safe. I recognize that there are additional issues that require further debate. For example, some who participated in our review, as well as some in Congress, would like to see more sweeping reforms to the use of National Security Letters, so that we have to go to a judge before issuing these requests. Here, I have concerns that we should not set a standard for terrorism investigations that is higher than those involved in investigating an ordinary crime. But I agree that greater oversight on the use of these letters may be appropriate, and am prepared to work with Congress on this issue. There are also those who would like to see different changes to the FISA court than the ones I have proposed. On all of these issues, I am open to working with Congress to ensure that we build a broad consensus for how to move forward, and am confident that we can shape an approach that meets our security needs while upholding the civil liberties of every American. Let me now turn to the separate set of concerns that have been raised overseas, and focus on America's approach to intelligence collection abroad. As I've indicated, the United States has unique responsibilities when it comes to intelligence collection. Our capabilities help protect not only our own nation, but our friends and allies as well. Our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy too. And the leaders of our close friends and allies deserve to know that if I want to learn what they think about an issue, I will pick up the phone and call them, rather than turning to surveillance. In other words, just as we balance security and privacy at home, our global leadership demands that we

balance our security requirements against our need to maintain trust and cooperation among people and leaders around the world.

For that reason, the new presidential directive that I have issued today will clearly prescribe what we do, and do not do, when it comes to our overseas surveillance. To begin with, the directive makes clear that the United States only uses signals intelligence for legitimate national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary people. I have also made it clear that the United States does not collect intelligence to suppress criticism or dissent, nor do we collect intelligence to disadvantage people on the basis of their ethnicity, race, gender, sexual orientation, or religious beliefs. And we do not collect intelligence to provide a competitive advantage to U.S. companies, or U.S. commercial sectors.

In terms of our bulk collection of signals intelligence, U.S. intelligence agencies will only use such data to meet specific security requirements: counter-intelligence; counter-terrorism; counter-proliferation; cyber-security; force protection for our troops and allies; and combating transnational crime, including sanctions evasion. Moreover, I have directed that we take the unprecedented step of extending certain protections that we have for the American people to people overseas. I have directed the DNI, in consultation with the Attorney General, to develop these safeguards, which will limit the duration that we can hold personal information, while also restricting the use of this information.

The bottom line is that people around the world – regardless of their nationality – should know that the United States is not spying on ordinary people who don't threaten our national security, and that we take their privacy concerns into account. This applies to foreign leaders as well. Given the understandable attention that this issue has received, I have made clear to the intelligence community that – unless there is a compelling national security purpose – we

will not monitor the communications of heads of state and government of our close friends and allies. And I've instructed my national security team, as well as the intelligence community, to work with foreign counterparts to deepen our coordination and cooperation in ways that rebuild trust going forward.

Now let me be clear: our intelligence agencies will continue to gather information about the intentions of governments – as opposed to ordinary citizens – around the world, in the same way that the intelligence services of every other nation does. We will not apologize simply because our services may be more effective. But heads of state and government with whom we work closely, and on whose cooperation we depend, should feel confident that we are treating them as real partners. The changes I've ordered do just that.

Finally, to make sure that we follow through on these reforms, I am making some important changes to how our government is organized. The State Department will designate a senior officer to coordinate our diplomacy on issues related to technology and signals intelligence. We will appoint a senior official at the White House to implement the new privacy safeguards that I have announced today. I will devote the resources to centralize and improve the process we use to handle foreign requests for legal assistance, keeping our high standards for privacy while helping foreign partners fight crime and terrorism.

I have also asked my Counselor, John Podesta, to lead a comprehensive review of big data and privacy. This group will consist of government officials who—along with the President's Council of Advisors on Science and Technology—will reach out to privacy experts, technologists and business leaders, and look at how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security.

For ultimately, what’s at stake in this debate goes far beyond a few months of headlines, or passing tensions in our foreign policy. When you cut through the noise, what’s really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed. Whether it’s the ability of individuals to communicate ideas; to access information that would have once filled every great library in every country in the world; or to forge bonds with people on other sides of the globe, technology is remaking what is possible for individuals, for institutions, and for the international order. So while the reforms that I have announced will point us in a new direction, I am mindful that more work will be needed in the future.

One thing I’m certain of: this debate will make us stronger. And I also know that in this time of change, the United States of America will have to lead. It may seem sometimes that America is being held to a different standard, and the readiness of some to assume the worst motives by our government can be frustrating. No one expects China to have an open debate about their surveillance programs, or Russia to take the privacy concerns of citizens into account. But let us remember that we are held to a different standard precisely because we have been at the forefront in defending personal privacy and human dignity.

As the nation that developed the Internet, the world expects us to ensure that the digital revolution works as a tool for individual empowerment rather than government control. Having faced down the totalitarian dangers of fascism and communism, the world expects us to stand up for the principle that every person has the right to think and write and form relationships freely – because individual freedom is the wellspring of human progress. Those values make us who we are. And because of the strength of our own democracy, we should not shy away from high expectations. For more than two centuries, our Constitution has weathered every type of change because we have been willing to defend it, and because we have been

willing to question the actions that have been taken in its defense. Today is no different. Together, let us chart a way forward that secures the life of our nation, while preserving the liberties that make our nation worth fighting for. Thank you.