As Prepared for Delivery

Thank you so much, Jeff, for that kind introduction and thanks to the American Enterprise Institute for your thoughtful, balanced work on cybersecurity in recent years.

Thank you, Michael Hayden. It is always a pleasure to share a stage with you on any topic.

As we continue our national conversation on what privacy means in the Internet age, I believe that we need to focus more on how privacy interacts with our security.

I reject the notion of "balancing" privacy and security. Privacy is not at odds with security; without security, there is no real privacy.

The concept of security as a necessary guarantee of individual rights is not a new one. John Locke theorized that men form governments in order to safeguard their lives, liberty, and property in a dangerous world. And in our digitally connected world, privacy is an empty letter without security.

Today, even mundane actions create vast amounts of digital exhaust – just think about the electronic activity you did on your way to AEI this morning. Did you set your alarm on your phone to wake up? Did you call Uber or a taxi through an on-line application? Did you plot the best way to get here on Google maps? Did you pay for your coffee at Starbucks with a credit card or a mobile app? How many emails and text messages have you already sent this morning? What data was mined from the content of those communications by both the sending and receiving applications? How many different mobile apps have used GPS to determine your exact location every step of the way? It's only 9 a.m. and already you've interacted with the Internet scores of times.

Without security, your ability to keep all of those digital bread crumbs from being public is meaningless. Malware could be lurking in your applications and services, sending all of your personal data to third parties. Without secure networks, Russian crime organizations can steal your financial data or Chinese hackers can steal your identity. Some of you in the room may be of interest to the Chinese, Russians, or Iranian governments, and their intelligence services are trying to collect your pattern of life to enable their next spear-phishing campaign against you or your co-workers.

Your ability to earn a living by engaging in free enterprise in the modern world relies on a secure Internet. Without a secure Internet, you can't start a business, obtain a loan, or make an investment online.

Only with these considerations in mind can we begin to determine what constitutes a reasonable expectation of privacy in the Internet age.

Some offer expansive, self-serving, and impractically vague definitions of privacy without any consequence or cost. They downplay the many, very real threats we face today and ignore the need for us to defend ourselves. Even if we did not live in such a dangerous world, our need for digital connectivity in nearly every aspect of our economy and our personal lives precludes an absolute level of privacy.

Some American technology companies demand a "code of conduct" when it comes to U.S. intelligence agencies accessing the Internet. Let me be clear, I believe in strong legal restraints and vigorous oversight of intelligence activities. We have both of those in volumes.

Perhaps those companies would do better to look inward at their own practices regarding data privacy. Maybe we should consider a code of conduct governing what these companies can do with the data they collect on their customers and sell for profit. Certainly that would advance the privacy goals they claim to value so highly.

If these critics had their way; if we put unnecessary restrictions on what NSA or the FBI can do on the Internet, who would defend the Internet and the critical infrastructure that depends on it from hackers working for criminals, terrorists, and hostile governments?

If we can use some of that digital exhaust that is provided to third parties and does not violate privacy law to detect and foil terrorist plots to conduct another mass-casualty attacks on U.S. soil, shouldn't we do it? If we can detect and foil dangerous cyber attacks, while protecting law-abiding Americans' privacy, shouldn't we do that too? We need to maintain strict rules about when and how the government can access metadata, but we shouldn't restrain our intelligence and law enforcement agencies from accessing data that's relevant to a serious crime or a national security threat.

I'm not suggesting we give the government unlimited authority—far from it—but we can't have meaningful security, and therefore meaningful privacy, without intelligence services that have the tools and authorities they need to do their job and keep America safe. The anonymous nature of the Internet doesn't allow for bright-line national boundaries, and innocent traffic is often co-mingled with the communications of terrorists, spies, nuclear weapons proliferators, and cyber criminals. We must—and do—have strong restrictions on when and how the government can access that co-mingled traffic, but we must also remember that reflexively curtailing the NSA will ultimately lead to less online privacy, less free enterprise, and less liberty—not more.

The courts will continue to have a role in this debate. The Supreme Court is free to revisit Smith v. Maryland, and it will continue to answer what the Fourth Amendment means on the Internet in the next few years. It may be time for Smith v. Maryland to be analyzed by the Court now that we are in the digital age. But let's

not forget what a fundamental shift—and impingement to business and the economy—it would be for the Court to find a Fourth Amendment protection in metadata handed freely to third parties. I'm not sure the Internet would continue as we know it.

For our part, we in Congress need to update the laws that govern intelligence and law enforcement access to Internet data, namely the Foreign Intelligence Surveillance Act, the Electronic Communications Privacy Act, and The Communications Assistance for Law Enforcement Act. As part of that debate, we need to consider how to modernize these laws to be technology neutral. If we bring everyone to the table, I believe we could do that in a way that satisfies our national security, law enforcement, and privacy demands.

When I say technology neutral, I mean we must ensure these laws focus on what data can be accessed, under what circumstances, and for what purpose, regardless of where that data is found and how it is stored or moved. If we don't, technology will keep shifting and changing and our laws will continue to lag behind in a way that is not helpful to either privacy or security.

FISA is a great example of this problem. In recent years we have made incremental changes to the law, under either the looming deadline of a legislative sunset or because a change in technology created a dangerous gap in our collection. These changes have added new layers to FISA's outdated 1970's-era technological framework.

Other laws like ECPA and CALEA may not be in the forefront of everyone's mind, perhaps because there are no looming legislative sunsets, but they are also hopelessly rooted in yesterday's technology. Only by modernizing these tools can we give our intelligence and law enforcement agencies the tools they need to keep us safe, and to protect the systems upon which every American relies.

The world remains a dangerous place, and two oceans are no longer much insulation from outside threats. The good news is that those who seek to do us harm are also dependent on digital connectivity, and they also leave a thick trail of digital exhaust behind them as they move and communicate. We need to keep working to find that exhaust, to find the relevant signal among all the noise on the Internet, and to do it in the least intrusive manner possible.

Improving tools and technology allow the NSA and FBI to get better every day at finding that signal without unnecessarily disturbing anyone's privacy. I wish there was a way for me to better convey to the American people how hard the men and women working at NSA and FBI work to get that right every day, and how badly they want to get it right every time. They deserve our trust and support, and it is vital that we work hard to ensure that they have updated tools and authorities to help them do their important work.

Unfortunately, over the past year, many have made careers and some have even been nominated for Pulitzer Prizes based on publishing incredibly misleading information and stories that often tell one or two pieces of a 1,000 piece puzzle.

A good example of this lack of context can be found in an oft-cited quote from Benjamin Franklin. In 1755, Franklin wrote a letter stating: “Those who would give up essential Liberty, to purchase a little temporary safety, deserve neither Liberty or Safety.”

This phrase is often repeated by those who suggest the federal government is out of control. However, the quote is irrelevant to privacy issues like anonymous phone call metadata. Franklin was weighing in on a political struggle over the authority to levy taxes between the Pennsylvania Assembly and the colonial governor during the French and Indian war.

The Assembly wanted to tax the lands of the Penn family to fund defense against French and Indian attacks. The governor, appointed by the Penn family, kept vetoing those taxes. The governor wanted the assembly to renounce its tax authority in exchange for him ensuring defense of the frontier. Franklin referred to the Pennsylvania Assembly’s right to levy taxes and their right to self government, not an absolute liberty from government.

This lack of context and disinformation has been common in the past year of sensationalist coverage over so-called “domestic spying” or “rogue agencies.” Those who seek to mislead present a false choice that I reject completely. It is critical that policy makers take the time, as we did recently with the USA Freedom Act, to understand facts and ensure changes conform to reality.

As we struggle with these important questions about how privacy and security interact, it is clear that at the end of the day, privacy and security are not in conflict – instead, privacy is nothing without security. And we should vigorously pursue both.

Thank you very much again for the invitation; I look forward to the discussion and your questions.