**RightsCon Speech**
**Sen. Ron Wyden**
**March 30, 2016**

Thanks for having me. I am here to tell you why I will use every power I have as a senator to block plans to weaken strong encryption. I am here to tell you why FBI Director Comey's plans and expected legislation will be a lose-lose - they would lead to less security and less liberty. And I am here to ask you to join me in offering a win-win alternative, what I call a "New Compact for Security and Liberty."

And let me be clear at the outset that the debate about data security is not about choosing security or choosing privacy. It is about choosing less security or choosing more security. People who think that the government should have more surveillance powers will often try to frame this debate as a choice between privacy and security. They are wrong. Our job is to convince the public that when politicians or the news media say that, we are here to tell you it's not the case. It's less security versus more security.

In the wake of virtually every tragedy, too many politicians and high-ranking intelligence and law-enforcement officials insist they need new powers, because new invasions of our private spaces are needed to keep us safe. That overreach led to secret mass surveillance under the Patriot Act, warrantless searches for Americans' emails, and the current fight to weaken encryption, which is a long way from over.

Secret mass surveillance was proven to be a loser, warrantless email searches will be proven to be a loser and plans to weaken strong encryption are a double loser.

So while I respect our law-enforcement officers and want to give them the tools they need to do their jobs, I will oppose any effort to undermine the privacy and security of individual Americans.

Today, I want to refocus the debate on how to have policies that are win-win: that produce more security and more liberty. I'll share my ideas about how to get there. But first, I want to explain why this fight is so important.

THREATS TO PRIVACY

Here's what we need to explain to the politicians: today's threats to privacy are unlike anything we've seen before. Centuries-old technological limits that stopped governments from gathering real-time personal information about a

country's entire population are gone. Physical limits on government power have all but disappeared.

Bruce Schneier has called our era the "golden age of surveillance." In my view outdated laws and precedents, combined with advances in technology, have given government agencies a greater ability to peer into individuals' private lives than they've ever had before. And despite what the FBI Director and other officials say about "going dark," on balance government agencies' surveillance capabilities are at an all-time high. With all of the internet-connected devices on our persons and in our homes, for most Americans there is literally nowhere in our lives the government isn't capable of reaching. There are very, very few places we can expect real privacy, not even our most personal spaces. Even our very thoughts often end up recorded on the technology we carry.

For centuries, individual liberty was protected by technological limitations. Gathering real-time personal information about a country's entire population was impossible. It would have required more resources than any government could muster. A few repressive regimes like East Germany and the Soviet Union tried hard to achieve this, and actually spent the time and effort to build sprawling networks of spies and informants to monitor their own citizens. It was an understanding of that authoritarian impulse within all governments and the inevitability of technological change that caused George Orwell to issue the warning of 1984. Almost 70 years later, technology has caught up with Orwell's imagination. Your television screen can indeed watch you, along with more and more gadgets that we wear, carry or live with every day. Governments around the world now have the technological capability to collect files on every single citizen that would put the Stasi's work to shame.

**Our laws, our courts, and our entire system of government were designed by the Founders to protect individual liberty from the power of the state. They were also all designed with the understanding that there were many things that government could not physically do. The Founders understood that power should not be trusted. They wove checks and balances on the power of the state into the fabric of our institutions. They relied on the physical limitations on the state's power for the times when institutions failed. Now those physical limitations have largely disappeared. Our country must stay true to the Founders' intent and establish new laws and precedents, so that individual liberty is guaranteed by more than just the goodwill of men and women in power.**

This is an exceptionally dangerous time for many of our fundamental freedoms, including freedom of expression, free association, and privacy. It is now technologically possible for the state to irretrievably encroach on these freedoms.

Let me be clear, I am not accusing government officials of deliberately setting out to restrict Americans' rights. It makes sense, within their jobs, that law-enforcement and intelligence officials want access to the most information about the most people, with the least hassle and inconvenience. What they do is important, but I believe security without liberty is not a choice a free people will make.

Fortunately, in America the FBI Director doesn't get to decide the rules for searching your phone, and the NSA Director doesn't get to write the rules for reading your emails. Our founders made sure of that. However, it is the responsibility of elected representatives to write new rules that protect individual security and liberty against any encroachment, and it is the responsibility of judges to question any increase in government power and to ensure that the protections of the 4th and 5th amendment are as real as in the day the Constitution was drafted.

**In this case, the rapid advances in technology over the past 20 years threaten the rights of every single American more immediately and more personally than most people fully understand. I'm depending on the people who understand that threat - <u>every one of you here today</u> - to spell out those dangers to the rest of the country.**

---

Your opponents will talk about "going dark" and "letting terrorists win", and I think it's important, in light of all of this talk about how the spread of encryption is some sort of national catastrophe, to step back and look at the situation in perspective. Critics of encryption have suggested that those of us who believe that American consumers' devices should be as secure as possible are "absolutists" who have taken a position that is so dangerous that it is "not sustainable."

**I think that it is useful to compare this discussion to another one that was playing out fifty years ago. Fifty years ago this summer, the Supreme Court handed down a landmark decision in the case of *Miranda vs. Arizona*, in which the Court ruled that before law enforcement officers interrogate a suspect, they must advise that person of his or her constitutional rights. Everyone who's ever watched a TV cop show knows this – you have the right to remain silent, you have the right to an attorney, and so forth. Today, this is a very important feature of the American justice system. It helps ensure that poor people know that they have the same rights under the law as rich people who can afford high-priced lawyers. And it helps reduce the likelihood of innocent people who are**

**unsure about their rights being pressured to sign false confessions. The *Miranda* ruling helped bring our country closer to the promise of equal justice for all.**

**But if you had been following the public debate back in the summer of 1966, you would have heard a lot of politicians and prosecutors saying that the sky was falling. A few weeks after the decision, a New York Times headline read "*Miranda* Decision Said to End Effective Use of Confessions." The article quoted some of the most respected prosecutors and law enforcement officials in the country warning that this decision was an absolute catastrophe. Future president Richard Nixon called the ruling a "Dickensian legalism" that would "hamstring" law enforcement, and he even suggested that the Constitution should be amended to overturn it.**

**Needless to say, the sky did not fall. In fact, crime rates have been dropping for the past twenty or thirty years. The national murder rate and burglary rate are both lower than they were the day that the *Miranda* ruling was handed down. Obviously there are a lot of factors that go into crime rates, but I think it's clear that despite all of the dire warnings from both politicians and respected law enforcement officials, this ruling did not lead to the end of law enforcement in America. Fifty years later, the *Miranda* ruling remains a cornerstone of American due process.**

Just as our justice system successfully adapted to the *Miranda* ruling, law enforcement and intelligence agencies are going to find ways to adapt and keep doing their jobs in the age of strong encryption. It has been suggested that strong encryption on smartphones will mean that "everybody is walking around with a Swiss bank account in their pocket." I would say in response that if you want to take a look at a criminal suspect's bank records, maybe you could try serving a warrant on his bank. Even the Swiss banks are forthcoming in this day and age. How's that for a radical suggestion?

The fact of the matter is that government agencies are going to continue to be able to gather information on suspects, even with the spread of strong encryption. If the government has evidence that you are up to something nefarious, they can go to your bank, they can go to your employer, they can go to all sorts of companies that you do business with. And that includes communications companies. Lots of communications companies are going to retain the ability to decrypt their customers' communications, in order to provide services like password recovery and antivirus scanning, or to show you ads so they can make their products free to use. And even communications companies that recognize the security risk to their customers of retaining such power will still have access to unencrypted metadata – like the address of the sender and the

recipient - which will offer enormous surveillance opportunities that didn't exist fifteen years ago and aren't going away anytime soon.

---

And it's worth noting that the spread of networked sensors and the Internet of Things is also creating even newer opportunities for surveillance, and new threats to the safety and security of ourselves and our families, every day.

Last month, an independent group released a report addressing the current debate about encryption policy. This group included some serious security experts, including a former Assistant Secretary of Defense, a former Assistant Attorney General, and the former Director of the National Counterterrorism Center. Their report was appropriately titled "Don't Panic." And here's how it concluded:

**"The increased availability of encryption technologies certainly impedes government surveillance under certain circumstances, and in this sense the government is losing some surveillance opportunities. However, we concluded that the combination of technological developments and market forces is likely to fill some of these gaps and, more broadly, to ensure that the government will gain new opportunities to gather critical information from surveillance."**

**It is true that strong encryption will sometimes mean that information on an individual's phone or computer will be beyond the government's reach. And it is equally true that this information will therefore be out of the reach of hackers and criminals who may want to do that individual harm. But it's worth remembering that fifteen years ago almost no one in America owned a smartphone. A lot of the information that is now stored on a person's phone used to be stored only in that person's head, where it was beyond the reach of any warrant. This information deserves protection, most importantly it deserves protection from ANYONE who could misuse it.**

I occasionally hear from people who say they aren't afraid of the government having their information, or listening in on their Amazon Echo, because they don't have anything to hide. To these people, I say I salute your faith in our government. But it wasn't all that long ago that J. Edgar Hoover was FBI Director. He amassed information about the private lives of politicians and civil rights leaders, and Hoover used that information to intimidate and harass anyone he viewed as a threat, including Martin Luther King, Jr. Now imagine J. Edgar Hoover had all of the information technology that is available today. What

political or social movements might you never have heard of, and benefited from, because someone like Hoover was able to use that power to bring them down?

There is a real cost to society when everyone KNOWS their most personal thoughts and conversations can be made public or viewed by authorities. There is a chilling effect, a self-editing of potentially controversial or unconventional statements. I know my email conversations are sometimes a lot less colorful than when I talk to someone face-to-face. With universal surveillance, that bleaching of thought and language could reach our most private conversations.

## New Compact for Security and Liberty In the Digital Age

So how do Americans protect our rights? Here's what I have been calling a New Compact for Security and Liberty in the Digital Age:

First, end this campaign against strong encryption. Encryption is one of the best defenses an individual has to protect himself or herself in the digital world. Without encryption, the technologies we live with would enable thieves to take not only our wallets and purses, but our entire life savings in the blink of an eye. Without encryption, connected technologies could be perverted to plan home invasions, abductions, and worse. Baby monitors and wi-fi enabled dolls have already been hacked. Cars have been hacked. Personal photos of the rich and famous have been hacked. Health records and credit cards and millions of sensitive government documents have been hacked.

Without encryption, the most personal affairs of every individual, whom they spend time with, where they go, and what they think could be laid bare despite their best efforts to keep that information private. Even with encryption, poor implementation and carelessness can leave an individual exposed, but encryption gives individuals a fighting chance at maintaining digital security in the modern world.

So I wrote a bill back in 2014, a simpler time, called the Secure Data Act. It is simple. It says the government can't require companies to weaken the security of their products. The Justice Department is trying to claim that the government has that power today. They dropped a high-profile case this week, but as sure as the night follows the day they will be back. So I need your help to pass the Secure Data Act into law.

## Strengthening Privacy Protections for Individuals

Second point: It's time to STRENGTHEN protections for the information individuals share with private companies.

I will propose to you today that one of our core principles should be that individuals do not lose their privacy rights just because they share some of their personal information with a particular company.

Most Americans now have relationships with a broad range of companies that store bits of personal information about them. This is a key feature of the digital economy. Consumers consent to share information with individual companies, and those companies tell their customers how that data will be handled. If a company violates the privacy rules in its terms of service agreement, it can lose business and even end up in court. As long as this whole process is sufficiently transparent to consumers, the market will help give people the privacy that they demand.

Here's the problem. A few decades ago, courts began ruling that if you provide information to a third party, like your bank or your phone company, you are no longer keeping it private, and it is no longer protected under the Fourth Amendment to the Constitution.

There is a huge, glaring problem with that logic. When you share your information with a single private company,that is not the same thing as making it public. Your phone company may have records of who you call, and your bank may have records of how you spend your money, but your contract with them will have rules for when and how they are allowed to share that information. They are not allowed to just disclose it freely.

This is true in the digital world as well. When I post a handsome new profile picture on Facebook, or send out a tweet to tell people that I'm holding a town hall in Oregon, I've chosen to make that information public. But when I send an email to my wife, or store a document in the cloud so I can work on it later, my service provider and I have an agreement that my information will stay private. The premise in current law is that I have agreed to make that information public just because my service provider is holding it. And that premise is simply absurd.

Supreme Court Justice Sonia Sotomayor addressed this issue in an opinion in 2012. I'd like to read what she said, because she summed the situation up very well.

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. …This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane

> tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the email addresses with which they correspond to their Internet service providers; and the books, groceries and medications they purchase to online retailers.

She went on to say that she would not assume that all information voluntarily disclosed to someone for a limited business purpose has lost its Fourth Amendment protections. And I couldn't agree more. It's time to recognize that when people provide information to a particular company, with an agreement that the information will not be made public, those people have not waived their privacy rights.

Third on the New Compact: Congress should adopt and announce a schedule to hold more open hearings to examine the privacy impacts of surveillance laws, authorities and practices. Right now a member of the Intelligence Committee might get a half an hour a year to ask questions in open session about the topics we're talking about today. Transparency and open discussions would bring the American people into this debate. Those moves are long overdue.

Fourth: Defenders of digital rights need be on the alert for attempts to undermine those rights without anybody noticing. Here's an example: right now the Justice Department is seeking a change to Federal Rule of Criminal Procedure 41, about how agents get warrants to track computer hackers. Specifically, they are asking to use a single warrant to remotely access any computer that a suspected hacker is believed to have broken into. This rule change could potentially allow federal investigators to use one warrant to access millions of computers, and it would treat the victims of the hack the same as the hacker himself. The rule change will go into effect later this year unless committed people mobilize to stop it. I'm going to be working hard to mobilize opposition to it, and I hope that many of you will join me in that effort.

Fifth: it is important to recognize that advances in technology do create some legitimate challenges for our intelligence and law-enforcement officials. And it is possible to help them adapt and develop new investigative methods without tossing our fundamental freedoms in the trash can. Now, I don't know if the FBI is here today, or if they're listening in to this. But here's what I know for sure. They ought to be hiring more people like those in this room.

## Conclusion

We can win this fight for security and liberty. It obviously won't be easy, but we've done it before. Remember in the January of 2012, we were talking about the anti-Internet SOPA and PIPA bills. The first vote was on whether to override my hold on PIPA. Talk about long odds. The Chamber of Commerce, Hollywood, all the

powerful special interests were against us. When that debate started, no one gave us a chance. Then the Internet community mobilized. Websites went dark in protest. And when the dust settled, well, everyone here knows how that ended. We won. Let’s work together and do it again.