**Remarks of Senator Ron Wyden at the TechFestNW Conference**
**"Standing Up for American Innovation and Your Privacy in the Digital Age"**
**As prepared for delivery**

I'm here to discuss promoting innovation and personal privacy in the digital age.

These are two concepts that I spend a lot of time thinking about, and I know that they are both very important to many of the people here in this room. A little heads up: as part of that analysis, I've concluded that securing innovation and privacy in the 21st Century requires reforming a decades-old legal rule known as the "Third-Party doctrine" so that when an individual shares their information with a person, business or institution, they no longer automatically lose all their privacy rights.

But before we plumb the depths of the Third-Party doctrine, I'd like to begin with a little long-term perspective.

For centuries, individual privacy was protected to a large extent by the limited resources of governments. It simply wasn't possible for governments to secretly collect huge amounts of personal information about every single citizen without building massive networks of spies and informants.

Not that some didn't try. A handful of repressive regimes like East Germany and Soviet Russia actually did this. By some counts the Stasi had more than 100,000 people watching targets through binoculars, planting bugs, children spying on their parents and neighbors spying on each other. This pervasive surveillance had an extraordinarily corrosive and destabilizing effect on those societies over time. Luckily, this sort of massive, dragnet surveillance was more the stuff of novels than reality for the citizens of most nations in the 20th century.

**Our luck has run out.** Here in the 21st century, this dynamic has already shifted in a profound and fundamental way. Advances in technology have made it possible for governments around the world to vacuum up and rifle through the personal information of huge numbers of law-abiding citizens.

If you would defend a society built on the principle of individual liberty you need to recognize that you can no longer rely on the fact that mass surveillance is hard – **in the 21st century, it's easy**. The only protections that we can count on now are those that are written into law, upheld by a responsible judiciary, and enforced by a public willing to stand up for their own freedoms.

Fortunately, our Founding Fathers left us with some pretty darn good legal principles that can guide us when it comes to privacy. The Fourth Amendment guarantees the fundamental right of the people to be secure from unreasonable searches and seizures. Justice Louis Brandeis called this the right to be left alone.

This is the right to be confident that our government will not arbitrarily enter our homes and search our closets and bedrooms and seize our belongings, the way that British officials did in colonial times. And it is our right to communicate privately with one another, without having that communication searched or seized without due process of law.

If our government wants to search your house or open your mail, the Constitution requires the government to go to a judge, show probable cause, and get a warrant.

These fundamental principles have served our country well for more than two hundred years. So the task before us is to figure out how to ensure these principles are upheld in the digital world.

This task is actually pretty straightforward if we keep a few key principles in mind. In America, the law is not, and should never be, written for the convenience of the government. To the extent changing

technologies present new challenges regarding privacy, they should be challenges for our government and its agents, not the individual.

As such, the same protections that apply to your personal papers, conversations and correspondence in the physical world must, by default, protect your privacy in the online world.

What is new and distinctive about our era is that private companies now often hold large amounts of data about their customers. This is part of the technological revolution that allows me to carry far more than the sum of Thomas Jefferson's library and Ben Franklin's papers in the palm of my hand.

If only this revolution could grant us the wisdom Jefferson applied to the protection of the individual against the overbearing power of government.

Here's how I see the new realities. Individuals now consent to share information with companies under mutually agreed upon terms. If a particular company were to violate those terms it would risk ending up in court, and low barriers to market entry ensure that its customers would soon take their business elsewhere. Market forces can provide a powerful means for people to get the privacy that they demand.

While more can and should be done to assure that both sides in this transaction understand their rights and responsibilities, one thing is certain: there are only two parties to these transactions, the business and the individual. I believe the government should have no special rights in this new reality.

**Third-Party Doctrine**

I consider that common sense. Unfortunately, many of those whose job it is to carry out our laws are using shortcuts attached to old technologies and old ways of doing things to make their jobs easier and make protecting your privacy much, much harder.

Decades ago, in a series of decisions made by judges who did not fully understand 20th Century technology, much less anticipate the technology we have today, courts made law that took ordinary commercial transactions, like phone calls or a bank deposit, out of the protection of the Fourth Amendment. The courts' rationale for this third-party doctrine was that by dialing a number and conveying it to your phone company, or by sharing financial information with your bank, you were giving up any expectation of privacy. And under this 'Third-Party doctrine,' the records of that call or that deposit now became business records available to the government without Fourth Amendment protections.

Some will still argue that by sharing data freely with Facebook, Google, Mint, Uber, Twitter, Fitbit, or Instagram, Americans are choosing to make that data public. But that is simply not the case. I might not have any expectation of privacy when I post a handsome new profile picture on Facebook, or when I send out a tweet to tell people I'll be at the Tech Northwest conference. But when I send an email to my wife, or store a document in the cloud so I can review it later, my service provider and I have an agreement that my information will stay private. Neither of us have invited the government to have a peek. Basically, I think sharing this information with Google is like putting property in a safety deposit box, but the government thinks I'm posting it on a billboard out on I-5.

Citizens have agreed to a contract with Google or Mint that keeps their email or financial data private. In many cases these companies don't even know what information they're holding for you. Making information available to a service provider for a limited business purpose - so that they can give you a new app, or provide targeted ads, or do any other kind of business with you - is simply not the same as broadcasting that information to the public. In the view of the law this data **should** be as secure to your person as if it were sitting in a locked filing cabinet in your home office.

Even if one is inclined to agree with the reasoning behind these flawed court decisions, it is indisputable to me that they have not kept up with the times. When the Smith v. Maryland case was decided in 1979, an individual might use many different phones each day to make calls. Today, you will likely use just one. Those phone records, when combined with email, texts, pictures and web activity all contained on your cell phone now document the vast majority of your interactions with the world. No reasonable judge would have deliberately given the government warrantless access to this trove of private data and it's time that the law reflected this reality. It is time to reform outdated legal doctrines and laws to reflect both the constitution and public expectations.

Supreme Court Justice Sonia Sotomayor addressed this issue head-on in an opinion from 2012. She wrote:

> "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. "

The Judge added 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 don't think anybody else should assume that either. It is 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. I believe it is time for policymakers and courts to make that judgment as well.

**A Path Toward Reform**

So, if all of you and I are serious about this goal, and we agree that it is time to toss this outdated legal doctrine on the junk heap and replace it with an updated framework that adheres to the values of the Founding Fathers, protects individual privacy, and promotes innovation, where do we start?

I've served for thirteen years on the Senate Intelligence Committee, so one place that I'd like to start is with updated rules for America's intelligence agencies. Those of you who follow the news closely will know that the Senate is now considering a serious overhaul of the domestic surveillance statute known as the Foreign Intelligence Surveillance Act. There's still a lot of work to do, but I'm encouraged by the direction that this debate is heading.

I believe that any serious effort to reform this law needs to end the bulk collection of Americans' personal information, starting with their phone records. I have been challenging this program for years on the grounds that isn't just harmless old metadata. Furthermore, I believe that Congress needs to reform the Foreign Intelligence Surveillance Court, to make it more transparent and to include an advocate for the American people. Additionally, there needs to be much greater transparency from intelligence agencies about the scale and scope of domestic surveillance activities, and private companies should be given the ability to disclose much more information about requests they receive from the government. Most of all, Congress must close the loophole that intelligence agencies are currently using to read a significant number of Americans' communications without a warrant.

If Congress can do all that it will be a great start for intelligence reform. And it will go a long way toward restoring confidence in America's technology brand, where our digital services are the envy of the world. That confidence has been significantly shaken by revelations about excessively broad NSA, FBI

and CIA surveillance. The next step will be to seriously examine collection that is done overseas. When the Foreign Intelligence Surveillance Act was written in the late 1970s, it was written to only apply to collection done inside the United States. But that was back in an era when each country essentially had its own separate communications infrastructure.

Now those separate systems have been replaced by an integrated global communications network, in which calls and emails within one country might be routed through multiple different countries. When you combine that shift with new technology that makes it much easier to obtain large amounts of data, it no longer makes sense to assume that collection done overseas will not sweep up the communications of large numbers of law-abiding Americans.

This means that the rules that govern collection overseas will need to be substantially revised. These are governed by something called Executive Order twelve-triple-three, which is more than 30 years old and predates this sea-change in global communications. I was encouraged a few weeks ago when the Senate Intelligence Committee recognized this fact, and voted to advance a bill that would begin to establish some firmer rules in this area.

It will also be important to reform law enforcement authorities as well.

For example, most people may not realize that the federal law governing law enforcement access to email, known as the Electronic Communications Privacy Act was written back in 1986, so it assumes that any email that is still sitting in your inbox after six months has been abandoned. I see a couple gray-haired techies in the crowd who can probably explain that one to the younger folks that are scratching their heads. 20th Century laws aren't going to cut it for 21st Century expectations.

And there are a number of other laws that need to be updated to keep pace with advancing technology. In particular, I believe that the laws governing the electronic tracking of individuals' movements and whereabouts need to be overhauled and modernized, and I'll come back to that in a minute.

It will also be important to further clarify the relationship between surveillance authorities used for law enforcement and those used for intelligence-gathering. I have certainly supported efforts to bring down unnecessary barriers to information-sharing between law enforcement and intelligence agencies. But it is also important to have clear rules about when information gathered using intelligence authorities can be used for non-intelligence purposes.

The various reforms that I have just laid out would all help rein in intelligence and law enforcement agencies that too often have been acting outside our Constitutional protections, particularly the Fourth Amendment. And this principle should be applied even further. All federal legislation must recognize that changing technologies should empower the individual, and not empower the state at the individual's expense - technological progress should never weaken the rights upon which our nation is built.

**Closing**

There is no question it is a dangerous world out there where America faces real threats and there are those who do not wish us well. Intelligence and law enforcement agencies have a vital role to play. The vast majority of the professionals at these agencies are hard working men and women who make enormous sacrifices to protect national security and public safety. And I think it's fantastic that advances in technology have given these men and women new tools. But new tools require new rules. And applying the Founding Fathers' principles to the age of high-tech digital surveillance is also going to require some new thinking.

Along those lines, I'll make a quick plug for a bill that I've introduced along with a Republican congressman from Utah named Jason Chaffetz that we call the GPS Act. This bill would establish new

rules for the use of location-tracking technology. Specifically, it would say that if the government wants to get an individual's location information from a private company, the government needs to show probable cause and get a warrant or emergency authorization. It would permit private companies to obtain and share their customers' location information with the customers' consent in the normal course of business, but it would prohibit private individuals from using tracking technologies if this consent is not given.

For example, right now if a woman's ex-boyfriend secretly taps her phone, he is breaking the law. Our bill would also make it a crime to hack her smartphone and track her every move. And I believe that will help a lot of domestic violence victims in particular rest easier.

So, TechFest Northwest I hope this provides insight for how Americans can have both innovation and privacy in the digital era. Together we're going to have to construct and build out a new legal framework that demonstrates privacy and innovation are not mutually exclusive. This new framework isn't going to be built in a day, and this outdated doctrine about people waiving their privacy rights when they share personal information with private companies isn't going to be overturned overnight. It's going to take some time, and it's going to take a lot of work by a lot of people. Here at TechFest Northwest, let's begin that heavy lifting now.