Souter. He has argued four cases before the U.S. Supreme Court.

In 2011 and again in 2014, Kevin was appointed to the Advisory Committee on Appellate Rules by Chief Justice John Roberts. This is a signal honor, as the Presiding Officer knows. He is one of only 3 private practitioners on the 10-person committee.

Currently, Kevin serves as the chairman of his firm's appellate group and has been recognized by several national publications and organizations for his leadership in the legal field.

As the former solicitor general of Alabama, Kevin has proved to be an exceptionally skilled attorney. He understands and respects the law, and I believe he will be an asset to our Nation's judicial system as a Federal judge on the Eleventh Circuit. Moreover, the American Bar Association unanimously gave Kevin a ''well qualified'' rating to serve on the Eleventh Circuit—the highest possible recommendation they are able to give.

I am confident that Kevin Newsom will serve honorably and apply the law with impartiality and fairness, which I believe is required of all judges. I believe that President Trump has made the right decision in selecting Kevin Newsom to sit on the Eleventh Circuit. I am hopeful that later today my colleagues on both sides of the aisle will vote to confirm Kevin Newsom without any reservations.

Mr. President, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

RETURN OF PAPERS—H.J. RES. 76

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the papers with respect to H.J. Res. 76 be returned to the House of Representatives at their request.

The PRESIDING OFFICER. Without objection, it is so ordered.

ORDER OF PROCEDURE

Mr. MCCONNELL. Mr. President, I ask unanimous consent that notwithstanding rule XXII, at 2:15 p.m. today, the Senate proceed to the consideration of Calendar No. 178, the nomination of Christopher Wray to be Director of the FBI. I further ask that there be 4 hours of debate on the nomination, equally divided in the usual form; that following the use or yielding back of time, the Senate vote on confirmation of the nomination with no intervening action or debate; that if confirmed, the President be immediately notified of the Senate's action. I further ask that following disposition of the Wray nomination, all postcloture time on the Newsom nomination be considered expired.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

RECESS

The PRESIDING OFFICER. Under the previous order, the Senate stands in recess until 2:15 p.m.

Thereupon, the Senate, at 12:31 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. PORTMAN).

EXECUTIVE CALENDAR

The PRESIDING OFFICER. Under the previous order, the Senate will proceed to the consideration of the following nomination, which the clerk will report.

The bill clerk read the nomination of Christopher A. Wray, of Georgia, to be Director of the Federal Bureau of Investigation for a term of ten years.

The PRESIDING OFFICER. There will now be 4 hours of debate equally divided in the usual form.

The President pro tempore, the Senator from Utah, is recognized.

INTERNATIONAL COMMUNICATIONS PRIVACY ACT

Mr. HATCH. Mr. President, I represent a generation of lawmakers brought up on the principles of bipartisanship and compromise, and I believe these very virtues are the key to my success as a legislator. By putting these principles in practice as chairman of the Finance Committee, I was able to pass more than 40 bills into law during the last Congress, and by working with my friends across the aisle over many decades of public service, I have been able to pass more legislation than anyone alive today.

I draw from these personal experiences to illustrate a simple point: In an era of endless gridlock and increasing polarization, there is no alternative to civility and healthy debate. We would do well to remember this in light of the frustrations we have all felt over the past several months.

The Senate is capable of so much more than it is today. I know because I have seen the Senate at its best, and I have seen the Senate when regular order was the norm, when legislation was debated in committee, and when Members worked constructively with one another for the good of the country. I have seen the Senate when it truly lived up to its reputation as the world's greatest deliberative body.

I believe we can again see this body at its best, but restoring the Senate to its proper function requires real change on all sides. It begins by recognizing that all of us here, Democrats and Republicans alike, are to some extent culpable for the current dysfunction. If we want to break free of the current gridlock and if we want to show the American people we are serious about legislating, then we have to be honest with ourselves, and we have to recognize that laying all the blame on the other side is as counterproductive as it is disingenuous.

Most importantly, we must be willing to work in good faith with Members of the opposite party. All too often, we miss the opportunity to effect meaningful change by hiding behind partisan differences. We must take the opposite course by renewing our efforts to reach across the aisle to overcome division and forge consensus. There is no better template for effective, bipartisan legislating.

This is the model I have followed for decades for the betterment of Utah and the Nation, and it is the model I have followed most recently in working with my dear friend Senator COONS to introduce the International Communications Privacy Act, or what we affectionately refer to as ICPA.

ICPA is more than just a commonsense proposal that updates law enforcement for the modern age; it is a symbol of what our two parties can accomplish when we lay aside petty differences and come together for the good of our Nation. In crafting this proposal, Senator COONS and I took great pains to strengthen international data privacy protections while also enhancing law enforcement's ability to access data across borders.

This issue has long been a priority of mine. I have spoken about it at length both here on the Senate floor and in other venues and have introduced legislation on the subject over multiple Congresses. Most recently, I came to the Senate floor to explain how the rise of cloud and remote network computing has transformed the way we store data and to describe the implications of that transformation for our data privacy laws.

Until relatively recently, most electronic data was housed in personal computers or on servers located in offices or homes. This meant that in order to access data, a person could simply go to the relevant location and retrieve it. That is no longer the case. Nowadays, much of our data is stored not on home or office computers but in the cloud—a network of remote servers spread throughout the world that allows us to access data from literally anywhere. Data pertaining to a single individual or even to a single document may be stored at multiple sites spread across countries or even continents.

This has profound implications for data privacy. To begin with, our privacy laws require government officials to obtain a warrant before they can access many types of electronic communications. Warrants, however, traditionally have stopped at the warrant's edge. This means that if a law enforcement agent is investigating a crime here in the United States but a key piece of information is stored on a remote server outside the United States, the agent may have significant difficulty obtaining the information. Without a warrant or the ability to get a warrant, the agent may have to use diplomatic channels to obtain the information—a process that can be extremely slow and cumbersome.

Our privacy laws also prohibit disclosure to foreign entities. This means that when a foreign government is investigating a crime within its borders and a key piece of information is stored in the United States, the foreign government must likewise work through diplomatic channels to obtain the information.

The growing prevalence of cloud and remote network computing has put law enforcement into increasing conflict with these sorts of restrictions. Crime knows no borders. A child pornographer in Bangalore may post photos of an American victim on a British server which can be accessed worldwide. A U.S. official investigating the crime may need information stored on the British server in order to track down the culprit. If the server was in the United States, the official could simply issue a warrant. But that tool isn't available in this scenario because the server is overseas.

Moreover, the United Kingdom may have a statute, similar to our own law, that prohibits British service providers from disclosing communications to foreign entities. Diplomatic channels exist for sharing such data, but these channels are exceptionally slow and can take months or even years to process requests. In the meantime, crimes go unpunished and perpetrators disappear.

This state of affairs is simply not tenable. We cannot allow outdated laws to hamstring law enforcement efforts in this way. At the same time, we must adequately protect Americans' privacy against unwarranted government intrusion.

Some have suggested that the answer is to simply extend the reach of U.S. warrants worldwide. This, however, is not a viable solution as foreign disclosure laws can and do conflict with U.S. laws. Extending the reach of U.S. warrants without reasonable limits would thus place service providers in the impossible position of having to choose which country's laws to violate—ours or the foreign jurisdiction's.

What we need is a sensible regime with clear rules that determine access based on factors that matter to the person whose data is being sought. At the same time, we need to take proper account of the laws and interests of other countries, especially our allies.

We ought to avoid, wherever possible, trampling on other nations' sovereignty or ignoring their own citizens' legitimate claims to privacy. Accordingly, ICPA sets clear rules for when and how U.S. law enforcement can access electronic data based on the location and nationality of the person whose data is being sought.

Here is what the bill says:

If a person is a U.S. national or is located in the United States, law enforcement may compel disclosure, regardless of where the data is stored, provided the data is accessible from a U.S. computer and law enforcement uses proper criminal process.

If a person is not a U.S. national, however, and is not located in the United States, then different rules apply. These rules are founded on three principles: respect, comity, and reciprocity.

First, respect. If U.S. law enforcement wishes to access data belonging to a non-U.S. national located outside the United States, then U.S. law enforcement must first notify the person's country of citizenship and provide that country an opportunity to object. This shows respect to the other country and gives it an opportunity to assert the privacy rights of its citizen.

Second, comity. If, after receiving notice, the other country lodges an objection, a U.S. court undertakes a comity analysis to determine whose interests should rightly prevail—the U.S. interests in obtaining the data or the foreign interests in safeguarding the privacy of its citizen. As a part of this analysis, the court considers such factors as the location of the crime, the seriousness of the crime, the importance of the data to the investigation, and the possibility of accessing the data through other means.

Third, reciprocity. In order to receive notice and an opportunity to object, the other country must provide reciprocal rights to the United States. This ensures that the U.S. provides its own citizens an equal or greater level of protection against foreign requests for data. It also offers incentives to foreign governments to properly safeguard the data of U.S. citizens within their borders.

Up to this point, I have been focusing on requests by U.S. law enforcement for data stored outside the United States, but there is another side to the problem, and that is what happens when foreign law enforcement requests data stored inside the United States.

As I have mentioned, our privacy laws prohibit disclosure to foreign entities. Suppose a British subject committed a crime in Britain but data relevant to the investigation is stored in the United States. Even if British law provides for extraterritorial process, a UK official investigating the crime will be unable to obtain the data because U.S. law prevents disclosure to foreign officials. As with U.S. requests for data in other countries, diplomatic channels exist for sharing such data, but these channels are slow and extremely cumbersome.

Accordingly, for the past several months, I have been working with Senator GRAHAM and others to find a solution for this second part of the problem. Senator GRAHAM, together with Senator WHITEHOUSE, convened a hearing in May of this year that I believe highlighted the need for action. I have also met with Ambassadors and other high-ranking foreign officials who have impressed upon me the challenges they are facing under existing U.S. law.

I think we need to address this second side of the problem—foreign requests for data in the United States—as well. We need to address it in conjunction with the first side—U.S. requests for data in other countries.

It will not do to give foreign authorities readier access to data stored in the United States without likewise clarifying U.S. law enforcement's ability to obtain data stored abroad. Similarly, it is inconceivable to me that we would open our doors to foreign law enforcement requests while telling U.S. law enforcement that data in other countries is off-limits. Surely, we should not prefer foreign criminal investigations over domestic ones.

I believe these two issues—ICPA and the bilateral United States-United Kingdom agreement—are inextricably linked. I have worked in good faith with Senator GRAHAM and with Senator WHITEHOUSE to find a path forward on these issues. It is my firm belief that we need to move these two issues together. Everyone has a vested interest in privacy, and everyone has a vested interest in bringing criminals to justice. We are going to work together on this.

In closing, I would emphasize one additional point. The question of whether, when, and under what circumstances the United States should authorize law enforcement access to data stored abroad is a question for Congress. There have been suggestions in some corridors that this is a question for the courts to decide. I emphatically reject that question. This is a policy question for Congress.

We should not defer to the courts' interpretation of a statute that was passed 30 years ago with no thought or comprehension of the situation we face today. Subject to constitutional constraints, it is Congress's job to set the bounds of government's investigatory powers. We decide what government officials can and cannot do. We should not pass the buck to the judiciary merely because this is a complicated issue. We shouldn't do that.

The International Communications Privacy Act provides critical guidance to law enforcement while respecting the laws and interests of our allies. It brings a set of simple, straightforward rules to a chaotic area of the law and creates an example for other countries to follow. It is a balanced approach and a smart approach, and it deserves this body's full-throated support.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. THUNE. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

TAX REFORM

Mr. THUNE. Mr. President, when polls ask Americans what issues are most important to them, one topic seems to score high every time: jobs and the economy. It is not surprising. The American people have had a rough time over the past few years.