

our country, including the Federal Government, this information is not just troubling, it is terrifying, especially because there is no way for a single American to opt out of this collection or require notification that their information is being collected and stored.

Let me assure you, it is, and not only that, there is no way for Congress to have a say to exert oversight to take a closer look at what the CFPB is up to. One thing that is clear to me, every American deserves better than this, and after 5 years, I think it is safe to say we can do much better than this—and we better do much better than this—or we will have what the book “1984” suggested is going to happen.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. DAINES). The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

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 President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mr. PERDUE). Without objection, it is so ordered.

CYBER SECURITY

Mr. DAINES. Mr. President, the headlines in the past few months have been enough to paint a startling picture of how our Nation is handling technology and security these days.

Before I came to Congress, I spent 12 years working in the technology sector, but it doesn't take an extensive background in these fields to see that in the ever-changing realm of technology and online communication, America's constitutional freedoms and civil liberties are at risk and our security as a nation is under attack.

When it comes to protecting American citizens' privacy and personal information, we as a nation need to respond to the new threats our enemies are posing and the new tactics they are using and demand equal vigilance from those in our government who claim they have American safety at heart.

The modern battlefield is changing. We see it changing before our very eyes, and America needs to adapt. With the incredible advantages that modern technology offers, also with that come greater risks as well as greater responsibility. Our enemies, America's enemies, are utilizing social media in particular to recruit others to their side to plot against our rights, our freedoms, our American way of life.

As Michael Steinbach, the Assistant Director at the FBI's Counterterrorism Division, said to the House Homeland Security Committee just last month: “The foreign terrorist now has direct access into the United States like never before.”

We know for a fact that ISIS aggressively uses social media to spread its propaganda, to target individuals in our own country, and to urge them to attack us on our own soil.

In March of this year, the New York Times reported that ISIS's use of social media, including Twitter and high-quality online recruiting videos, has been “astonishingly successful,” and the speed at which modern social media moves means America must move faster.

In fact, we read about the recently foiled terrorist attack in Boston, where Islamic extremists planned to behead law enforcement officials. It shows us the importance of engaging these online terrorists, their propaganda machines, interpreting their encrypted communications, and cracking down on the spread of online terrorist networks—but how can we fight back against these cyber threats from abroad when our own government officials show themselves to be woefully incompetent?

We in this country spent months debating the National Security Agency's bulk collection of Americans' metadata, and in the meantime, while we are having this debate, Chinese hackers stole millions of Americans' personal information. In fact, it is estimated now those Chinese hackers broke into the Office of Personnel Management—basically the HR system of the Federal Government—and stole over 20 million records of employees of the Federal Government.

This recent breach of Federal employees' information may possibly be rooted in a phishing email. In fact, in a recent article in *Ars Technica* on June 8, they said:

It may be some time before the extent of the breach is known with any level of certainty. What is known is that a malware package—likely delivered via an e-mail “phishing” attack against OPM or Interior employees—managed to install itself within the OPM's IT systems and establish a backdoor for further attacks. The attackers then escalated their privileges on OPM's systems to the point where they had access to a wide swath of the agency's systems.

These hackers broke into the computers at the Federal Government's Office of Personnel Management. They were downloading the very forms Federal employees use to gain national security clearances.

In fact, earlier this month USA TODAY said:

The hackers took millions of the forms used by people to disclose intimate details of their lives for national security clearances. The information could be used to unmask covert agents or try to blackmail Americans into spying for an enemy.

In fact, I was one of those millions of Americans—as were other Members of Congress—whose personal information was compromised in this breach, and I demanded accountability from the Director and others at the OPM, but we also need to address the systemic problems with cyber security in this country directly.

The outdated security systems at the OPM and other agencies of the Federal Government recently hacked show that America is not up to speed with the kinds and the levels of cyber threats

our country is facing. Let me give an example. In the publication *Ars Technica* of June 8, 2015, it says:

The OPM hack is just the latest in a series of Federal network intrusions and data breaches, including recent incidents at the Internal Revenue Service, the State Department, and even the White House. These attacks have occurred despite the \$4.5 billion National Cybersecurity and Protection System program and its centerpiece capability, Einstein. Falling under the Department of Homeland Security's watch, that system sits astride the government's trusted Internet gateways. Einstein was originally based on deep packet inspection technology first deployed over a decade ago, and the system's latest \$218 million upgrade was supposed to make it capable of more active attack prevention. But the track flow analysis and signature detection capabilities of Einstein, drawn from both DHS traffic analysis and data shared by the National Security Agency, appears to be incapable of catching the sort of tactics that have become the modern baseline for state-sponsored network espionage and criminal attacks. Once such attacks are executed, they tend to look like normal network traffic.

Put simply, as new capabilities for Einstein are being rolled out, they're not keeping pace with the types of threats now facing federal agencies. And with the data from OPM and other breaches, foreign intelligence services have a goldmine of information about federal employees at every level of the government.

And this just at a time when the threats to our Nation are at very high levels.

The article continues:

It's a worrisome cache that could be easily leveraged for additional, highly-targeted cyber-attacks and other espionage. In a nation with a growing reputation for state of the art surveillance initiatives and cyber warfare techniques, how did we become the ones playing catch up?

But this isn't just about being sloppy or being slow; this is a matter of national security. America needs to get smart on cyber security and tech issues and to hold officials accountable for their behavior because there is just too much at stake if we fail. The American people will pay the price for a failure to adapt to this rapidly changing world of technology, this rapidly changing world of media, this rapidly changing world of information gathering, and for sheer carelessness on the part of those in authority.

Private sector innovation and progress can help America compete. As a member of the committee on commerce and having spent 28 years in the private sector—the last 12 years with a cloud computing startup which we took public and which became a great cloud computing company, with offices all over the world but based in my home State of Montana—I admit I had to smile when I saw that so many Congressmen want to regulate the private sector to protect the private sector from private threats. Well, again, in 28 years of serving in the private sector, I never once had my information breached. I never once had a letter from my HR department saying my information had been comprised. It wasn't until I became a Federal employee, elected to Congress a few years

ago, that my information was compromised. The private sector runs a whole lot faster than the public sector.

I think the government needs to look within to make sure we can be at the forefront of cyber technology and security, but these efforts will be thoroughly wasted if the Federal Government does not take the necessary precautions and procedures to protect the American people.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Alaska.

STRATEGIC PETROLEUM RESERVE

Ms. MURKOWSKI. Mr. President, I have come to the floor this evening to speak about our Nation's Strategic Petroleum Reserve, sometimes referred to as the SPR. It is a national security asset that has come into the news of late for a host of different reasons.

I am here this evening because of the concerns I have that others are potentially looking to our Strategic Petroleum Reserve—our strategic energy asset—as nothing more than a piggybank to fund some of the needs we have here in this Congress. I believe it is extremely shortsighted to raid our Nation's oil stockpile as an offset for the extension of the highway trust fund, and that is what we have had some conversation about today.

We had a vote earlier about whether to move forward on the highway trust fund. But as we have looked to find pathways forward for a multiyear highway trust fund reauthorization, which is something I support, it is important to know that not all pots of money are equal, that perhaps some are truly national security assets for which perhaps we need to show more considered respect.

I had an opportunity a few days ago—on Friday—to tour our Strategic Petroleum Reserve. I went to the Choc-taw Bayou site near Baton Rouge, LA. It was an opportunity for me to get a firsthand look at some of the challenges that currently face our four Strategic Petroleum Reserves that we have down in the Louisiana, Texas area and to have a better understanding as to their operational readiness. Quite honestly, it is a trip I wish more of our Members were willing to take because I think it would become clear to many the potential mistake we would be making in forcing the sale of billions of dollars of our emergency oil solely to pay for unrelated legislation. It is akin to selling the insurance on your house in order to pave your driveway. It just doesn't make sense.

For some, the Strategic Petroleum Reserve may be a very unknown national security asset. They do not really know what it is. But the SPR is our Nation's insurance policy against global energy supply disruptions. The Strategic Petroleum Reserve was established by law back in 1975 under the Energy Policy and Conservation Act, and its mission is twofold: to ensure

U.S. energy security by reducing the impacts of potential disruptions in U.S. petroleum supplies and secondly to carry out U.S. obligations under the international energy program.

We have about 700 million barrels of oil that are tucked away in underground salt caverns down in Louisiana and in Texas. We have a couple refined product reserves in other parts of the country, but our Strategic Petroleum Reserves are there in Louisiana and Texas. So if we have a major hurricane that takes out production in the Gulf of Mexico, as we saw with Hurricane Katrina back in 2005, we can turn to the SPR to help fill the gap. We did that in 2005. That is exactly the type of reason you would have the strategic asset.

But there are other times we have turned to the SPR. If there is a terrorist attack or a broader war disruption that alters the ability of other nations to send us oil, we can again turn to the reserve for help. We did this in 1991 with the Iraq war and then again in 2011 with the Libya supply disruption. So, again, when there was an emergency and we needed to ensure U.S. security, we had a ready reserve fund to turn to.

In the absence of policies that will allow our Nation to produce all of the oil it consumes every day, the Strategic Petroleum Reserve is really our best answer to the sudden absence of the energy we need, whether it is driving to work, whether it is powering our ships or our airplanes, moving our goods, or whatever that reason may be.

With the discussion we had today in terms of how we pay for this multiyear transportation bill, we are being asked to dramatically diminish the size of the Strategic Petroleum Reserve based again on the need to pay for the extension of the highway trust fund. It is totally unrelated—totally unrelated.

Those who would argue in favor of taking from the SPR, their argument is pretty simple. In fact, it is way too simple. They suggest that our international obligations require us to store enough petroleum to match 90 days of net imports. That is true. And they will say that given the growth we have seen in domestic oil production, we have enough now that we have a surplus within the Strategic Petroleum Reserve. Some have even suggested that an SPR is not even necessary anymore.

Well, I would be the first among us to suggest that changes need to be made to the Strategic Petroleum Reserve. Again, this was established back in 1975, and I think it is very fair to say the world has changed. It has changed dramatically since the 1970s. The global environment in which we are operating has changed dramatically. And the Department of Energy has said that today the impacts of an overall supply disruption of global oil markets would have the same effect on domestic petroleum product prices regardless of how U.S. oil import levels—or

whether U.S. refineries import crude from disrupted countries.

So there is a recognition that we have to get to modernizing the SPR. We have to ensure that we have right-sized it, that we are in alignment when it comes to moving oil from the Strategic Petroleum Reserve at those times we have determined are appropriate.

So I think it is important to know we are not just sitting still on this. The Department of Energy has begun work on a comprehensive, long-term strategic review of the SPR. We had good discussion about this when I was down in Louisiana on Friday with the Deputy Secretary of Energy, Chris Smith, talking about what this review will entail. It is looking at future SPR requirements regarding the size; regarding the composition of it; the geographic location—it has been suggested that perhaps there might be regional approaches; determining where we have chokepoints within the system in terms of distribution; how we move it; determining the impacts of what we see globally and what is happening with our own domestic production; and again being smart in how we are making sure we have right-sized the SPR and, in fairness, modernized the Strategic Petroleum Reserve.

We have a committee, as you know, Mr. President, that likes to roll up our sleeves and get into the weeds on making sure our policies are current and are relevant.

We need a deliberative process that will provide us with the proper understanding of the stakes and our options when it comes to how we handle our Strategic Petroleum Reserve. What we do not need—what we do not need—is an arbitrary process that picks a number. Right now, for purposes of the offset of what they are coming to the energy committee for, they are picking a number of—let's sell 101 million barrels of oil to fund a portion of the highway trust fund. Again, where is the connection between ensuring that we don't erode our national energy security assets?

I have said many times that the Strategic Petroleum Reserve is not an ATM. It is certainly not the petty cash drawer for Congress. We have a responsibility. A decision to sell substantial volumes of oil will increase our vulnerability to future supply disruptions at a time when we are still importing oil. We are importing about 5 million barrels a day.

Think about this. Think about the timing of this. It simply could not be worse. When you talk about volatility in the world, think about the news you read about today, what is happening in Iran, Iraq, and Syria. Now is the time for us to say that our national energy security assets are not that important; it is OK to nibble around the edges or worse and take significant amounts to put out on the market?

Let's consider a few facts to put things into perspective. First of all,