In fact, the GAO and the Federal Reserve inspector general both have warned about the need for increased security. Without full congressional oversight, how can we be sure this consumer data is secure? What kind of records does the CFPB keep? How would we know if it has been compromised? We have already seen the devastating effect of data breaches all over our Federal Government, and the damage it is doing to the American people across all sectors of our government, including the most recent OPM data breach, impacting millions of Americans and some of our intelligence assets abroad.

We have seen the potential exposure of extremely sensitive national security information. Also, we recently had a debate about privacy regarding the NSA metadata program. Many of my colleagues expressed outrage for the scope of the NSA program, even when the mission was protecting national security. We are now talking about an agency collecting massive amounts of personal consumer data, many times more data than the NSA program.

The CFPB's goal claims to be consumer protection. For all we know, this information they are collecting is even more susceptible to security threats and security breaches. If there is one thing we can agree upon, we need to make sure all Americans' personal information is safe and secure—especially from Washington. If some were upset about privacy in the NSA debate, we should certainly be paying attention to what the CFPB is doing with this personal information today.

Getting the CFPB under congressional oversight should not be a partisan issue. In order to protect consumers, we need to know what is going on in the very government agency tasked with protecting them. That is why we need to put in place more transparency—not less—more control, and more oversight. We can start by bringing the CFPB under congressional oversight immediately so we can actually protect consumers and stop the potential for abuse, fraud or identity theft.

While this agency was originally designed to protect consumers, one can only wonder how Washington's collecting so much personal information will actually protect us. I will be speaking much more on this topic as the weeks go by. Let it be said tonight, though, that on the fifth anniversary of Dodd-Frank, we are beginning to look at the unintended consequences of this rogue agency, the CFPB.

I yield the floor.

The PRESIDING OFFICER. The Senator from Wyoming.

DODD-FRANK ACT

Mr. ENZI. Mr. President, first, I would like to thank the Senator from Georgia for his outstanding comments. He is truly a great addition to this body and to the Budget Committee, where I have watched him go through numbers. I once mentioned that he knew how to balance the budget because he had been in business before, at which point he corrected me and said: In business, you don't get to just balance the budget. He is very correct on that.

We are at a point where we cannot afford to just balance the budget. We have to start paying down some of the debt if we expect our kids to ever be able to afford the interest. So I thank him for his comments. I am going to pile on with some more comments about some of those same things. I want to talk about what I have talked about several times over the past 5 years; that is the Dodd-Frank Act, which passed this body 5 years ago today, July 21, 2010.

This mammoth bill, which totaled 2,300 pages, has, 5 years later, led to many thousands of pages of rules and regulations. It is estimated that only 238 of the 390 rulemakings required by the law have been completed—millions of pages, and we still only have 238 of 390 rulemakings that the 2,300-page bill required. Theoretically, then, tens of thousands of pages of more regulations can be expected in the coming years—regulations that do not fix too big to fail, regulations that unduly burden our community banks and our credit unions, regulations that cover a host of industries that did not contribute to the financial crisis. And it does compromise the privacy of Americans.

I would like to take this opportunity to expand on these ideas. First of all, I would like to point out that I actually read the whole bill. I read it. I highlighted it. I put in colored tabs in different sections so I could refer to them easily. Then I talked to my colleagues, and I spoke on the floor to raise concerns about the bill roping in industries that did not cause the financial crisis, about the fact that it did not fix too big to fail. I raised a real ruckus about the creation of the Consumer Financial Protection Bureau, known as the CFPB, when they were trying to just kind of gloss over it and its ability to collect the financial information of American citizens without their consent.

I filed a simple amendment that would have required this Consumer Financial Protection Bureau to obtain written permission from consumers before collecting their information. Of course, my amendment was not allowed a vote and now the CFPB is collecting massive amounts of personal financial data. So here we are 5 years later, and hindsight has proven that many of the concerns I raised during the consideration of this bill were valid.

I have often said that knee-jerk reactions to legislative form have a very real danger of overcorrecting and causing a myriad of problems. In fact, some people say that if it is worth reacting to, it is worth overreacting to. That is exactly what happened here.

We did it through a comprehensive bill—2,300 pages. I do not like comprehensive bills. The purpose of comprehensive bills is so that they are incomprehensible, so that people cannot understand them. The best way to legislate is to take things in logical pieces and solve that problem in a way that all of America can come along with and understand.

Those problems are unintended consequences when they are in comprehensive bills. In correspondence and conversation with folks from Wyoming over the years, I have said that I treat all legislation the same. I read it and I consider both intended and what might be unintended consequences of the legislation. What I am here to talk about today are some of the consequences of the Dodd-Frank Act after 5 years.

First, there is the too-big-to-fail question. The Dodd-Frank Act was supposed to make it so American taxpayers would, according to President Obama, ''never again be asked to foot the bill for Wall Street's mistakes. . . . there will be no more tax-funded bailouts—period.''

Dodd-Frank increased capital requirements, it increased liquidity requirements, and it has been adding rules and new regulations steadily for the last 5 years. Folks who support the law would say all of those things are good things and make for a more secure financial sector. However, one of the contributors to too big to fail was the consolidation of banks and the financial industry, a byproduct of which was the reduction of the number of smaller community banks that serve small business owners, families, farmers, and ranchers, the people who actually know their customers. But thanks to the massive amount of rules and regulations, the Dodd-Frank has resulted in the compliance costs for community banks and credit unions going up significantly, and it increased the likelihood of consolidation. That fails the consumer.

Smaller community banks struggled to keep up with the flow of regulations and compliance costs. For example, since the passage of Dodd-Frank, the average compliance cost for larger institutions is about 12 percent of operating costs. For community banks, the cost to comply with the same regulations, a one-size-fits-all approach is 2½ times greater, or 30 percent of the operating costs. That is a big bite.

I was visiting some of those community banks and listened to them talk about the different regulations they now had to comply with. One of them had made this magnificent chart so that all of their loan officers could both follow along and make sure they got all of the parts of the procedure that this law had in regulation at that time. Now, they had to hire a compliance officer as well.

They had been able to handle that part themselves before. But after they explained all of this to me, I said: Now, let's see. My wife would kind of like to

expand the kitchen in our house. We have added onto it once before. If I wanted to get a loan from you, how long would it take me to get the loan? I said: I have a house in Gillette, and I have a house in DC, and I have both of them paid for. So we really do not have any outstanding debt. How long would that take?

They said: A minimum of 77 days. Then, of course, there would have to be an extra week so that if you decided it was not a good deal, you could undo the loan.

I wanted the loan. I wanted it 77 days before. I had to wait that long, and then there is a week for it. But here is another kicker that is in the bill. The Consumer Financial Protection Bureau has up to 150 days to tell me that I made a bad loan and cancel it. Hopefully, the construction would already be started by that time.

Well, I remember when I wanted to do that addition on the house. I went to my banker, and I explained to him what I wanted to do. It took me a whole day to get that loan—a whole day. Now, it is going to take 77 days, plus 1 week, and then I guess we have to wait 150 days to see if the Consumer Financial Protection Bureau is going to decide that they know better than I know.

My State of Wyoming is one of the most rural in the country. We had mostly community banks in Wyoming. I can attest that every visit I have had with banks in Wyoming since this law passed has had one main subject that remains constant: We are being crushed under the weight of these regulations. We are having to make tough choices about the services we provide.

Some of these banks are starting to consolidate with larger banks and become branches. Credit unions are not faring any better. According to the National Association of Federal Credit Unions, more than 1,250 credit unions have disappeared since the passage of Dodd-Frank. Of that number, over 90 percent had fewer than $100 million in assets, and the No. 1 reason they give for having to merge out of the business was the inability to keep up with the regulatory burden they face.

This is one unacceptable consequence of the Dodd-Frank law and one folks on both sides of the aisle should be appalled by. Now, equally appalling—maybe more appalling—is the importance the Dodd-Frank Act afforded to the agency it created, which the Senator from Georgia just talked about, the Consumer Financial Protection Bureau or the CFPB.

Now, this is an agency that really doesn't come under our jurisdiction; it actually works under the Federal Reserve and gets, I think it is up to 12 percent of the revenues of the Federal Reserve now, plus inflation. They will get up to 15 percent, plus inflation. We have no say over that. They don't report to us in any way, shape or form.

This agency has grown to over 1,450 employees. It has a facility whose offices' renovation budget has spiraled to over $216 million and faces almost no accountability to Congress. I don't have enough time allotted to talk about all the activities of the CFPB, but make no mistake, this agency's reach has increased exponentially over the past 5 years to the point where it is now taking enforcement actions covering telecommunications companies and has broadened its authority over the auto industry, which was specifically exempted from the CFPB in the Dodd-Frank bill.

Let me tell you how that happened. I did a bunch of speeches on the floor. I was interested in that third section. The first section was about the banks, the second was about hedge funds, and the third was about the new Consumer Financial Protection Bureau that wasn't going to have any control by anybody.

I found that little paragraph in there that said they have the ability to cancel a loan up to 150 days after the bank and the person—or whomever they are borrowing the money from—and the person receiving the money agreed to the loan. They can cancel it. I pointed that out in speeches.

One group of people listened to me. It was the automobile dealers. The automobile dealers flooded Washington with lobbyists, and they got an exclusion in the bill for automobile loans. That is the only exclusion in there. Of course, they are being retaliated against now for that, and I will talk about that in just a minute too. The CFPB issued a final rule on June 10 that would allow it to supervise nonbank companies qualified as larger participants of a market for automobile financing, along with a separate rule defining certain auto leases as a financial product or service.

What does this mean? It means the CFPB has expanded its oversight powers by saying: Oh, yes, auto leases are a financial product. They don't like what they did to us. It is a service, and we are allowed to regulate those. So we will just increase our level of oversight over this industry.

In fact, they have even taken a look at some of the loans that have been resold by automobile dealers and said those were discriminatory because they weren't the same. Well, when you go to the bank to sell a loan, you don't get the same deal every day, so that is really not discrimination, but according to this group that doesn't have any oversight over it, it is.

On the same day, the CFPB released its auto finance examination procedures for CFPB examiners to examine both banks and nonbanks. Keep in mind this is one example of hundreds of rules, enforcement actions, and other activities this agency is involved in across industries. Beyond increasing its incredible oversight reach, the CFPB has also engaged in massive data collection dating back to 2011. I spoke about this data collection, and the Senator from Georgia spoke about this data collection. I spoke about the data collection before the confirmation of Richard Cordray to be the Director of the CFPB on July 16, 2013. I was the only Senator to speak before this vote, and I repeated something I said during the debate of the Dodd-Frank Act that I think bears repeating again. On May 20, 2010, I said:

> This bill was supposed to be about regulating Wall Street; instead it's creating a Google Earth of your every financial transaction. That's right—the government will be able to see every detail of your finances. They can look at your transactions from the 50,000 foot perspective or they can look right down to the tiny details of the time and place where you pulled cash out of an ATM.

I talked about some of the data we had at that time. I am, unfortunately, going to expand on those comments because the CFPB continues to collect massive amounts of data without consent of the consumers.

The Government Accountability Office, GAO, is a nonpartisan, independent agency that investigates how the Federal Government spends taxpayer dollars. They released an extensive report on September 2014 detailing the data collection of the CFPB. Here is what they found.

Of the 12 large-scale collections they reviewed, three included information that identified individual consumers. The CFPB said those three collections weren't subject to the Dodd-Frank prohibition on collecting personally identifiable information.

What? The CFPB is collecting information on 700,000 auto sales per month, 10.7 million consumer credit reports per month, 25 million to 75 million individual credit card accounts, 29 million active mortgage loans, and 173 million total loans, as well as one-time collections of 5.5 million private student loans and 15 million to 40 million payday loans. This isn't the whole list, this is a sample rundown. Let's see, they are into the automobile sales, everything with your automobile sales, your consumer credit reports, your credit cards, your mortgage loans, your total loans, your student loans—and, if you do it, payday loans. Again, that is just a sample rundown.

Let's take a minute to let these numbers sink in. The CFPB collects information on 25 million to 75 million credit card accounts on a monthly basis. They want to be able to monitor 95 percent of all credit card transactions by 2016. I don't know about you, but this is highly disturbing, especially in light of the fact that the GAO report found that CFPB did not employ sufficient security and privacy protections to make sure this data remains safe.

In summary, the CFPB is collecting sensitive financial information on individuals by name, on millions of Americans, some of which has personally identifiable information that is supposed to be removed or not used, and they don't have the appropriate safeguard to protect this information.

Considering the increase in cyber attacks faced across different sectors in

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