DATA BROKERS - IS CONSUMERS' INFORMATION SECURE?

– – –

TUESDAY, NOVEMBER 3, 2015

United States Senate,

Committee on the Judiciary,

Subcommittee on Privacy, Technology and the Law

Washington, DC

The Committee met, pursuant to notice, at 2:47 p.m., Room 226, Dirksen Senate Office Building, Hon. Jeff Flake, Chairman of the Subcommittee, presiding.

Present: Senators Tillis, Whitehouse, Franken, and Blumenthal.

OPENING STATEMENT OF HON. JEFF FLAKE, A U.S. SENATOR FROM THE STATE OF ARIZONA, CHAIRMAN, SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

Senator Flake. The U.S. Senate Committee on the Judiciary's Subcommittee on Privacy, Technology and the Law will come to order. Thank you for your indulgence as we had the vote and appreciate you being here.

In recent years, data brokers have become an increasingly important sector of the economy, moved from traditional practices like credit reporting to providing complex risk mitigation services and targeted marketing for other companies.

As we generate more and more information through our daily activities, this information is sought by data brokers who seek to use it to help businesses and consumers make better choices. The brokering of data has become increasingly valuable, where it is estimated that they add over $100 billion in value to the economy.

Today, data brokers operate in nearly every sector of the economy, including the world of nonprofits. Nevertheless, while data brokers are an important part of the American economy, there are questions about their data storage and analysis practices; in particular, how is the information they collect and analyze used. It is

a matter of concern to privacy activists.

Today's hearing will ask the important question: How secure is the data collected by data brokers?

Now, to learn more about how secure personal data is in the hands of data brokers, we have brought together a panel of distinguished experts in data security and the data broker industry.

Pam Dixon is the Executive Director of the World Privacy Forum. Justin Harvey is the Chief Security Officer at Fidelis. I am also pleased that Frank Caserta, Acxiom's Chief Security Officer, has agreed to testify and will tell us what they are doing in this area.

You are going to hear the witnesses today. I hope this hearing, as well as future work in this area, will help us reach a point where we can say with confidence that the data broker industry is putting the attention and resources necessary to keep our data secure.

I will turn to Senator Franken for an opening statement. Then I will swear in and introduce the witnesses.

[The prepared statement of Senator Flake appears in the appendix.]

OPENING STATEMENT OF HON. AL FRANKEN, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Senator Franken. Mr. Chairman, I want to thank you for holding today's hearing on data brokers and the importance of data security.

In the last few years we have seen data breach after data breach affecting both public and private networks. It has become all too clear that we need to be doing more to ensure the security of Americans' personal information.

The cost of complacency is simply too high and it is absolutely appropriate, indeed, essential that we devote special attention to the security of particularly vast databases of sensitive consumer information like those compiled by data brokers, who boast that they have gathered extensive information about nearly every U.S. consumer.

Now, when we talk about data brokers today, I believe we are using the definition that the Federal Trade Commission, the FTC and others have recognized, referring to companies that are in the business of collecting information about people for the purpose of selling it to others for a variety of uses, including marketing and identity verification.

We are not talking about retailers that collect information about their own customers or employees, but companies that trade on the information of people with whom they generally have no direct relationship and no particular set of obligations.

That is important for a couple of reasons. It means that these types of companies are largely unknown to American consumers. The average American has probably never heard of companies like Acxiom, Datalogics, ID Analytics, and the many other data brokers that are out there, and the average American is almost certainly unaware of the largely unregulated space in which these companies have been operating while they have been amassing detailed information about individuals' lives.

Anything from online screen names and email addresses to Social Security numbers and credit card information or from political affiliations and histories of charitable giving to consumer purchase data, online search histories, medical conditions, and on and on and on.

But here in the Senate we cannot claim to be unaware. In recent years, reports by the Senate Commerce Committee, under the leadership of Senator Rockefeller, the Government Accountability Office, the Federal Trade Commission, as well as consumer groups, have been illuminating.

We know beyond a doubt that the threats data brokers' large databases pose for consumer privacy are real. Plainly, they are attractive targets for cyber criminals.

Just this September, Experian announced that one of its databases containing the records of 15 million consumers had been hacked and that the encryption of certain fields, like Social Security numbers, might have been compromised.

So the questions we turn to today are of the utmost importance. What are data brokers doing to prevent, detect and respond to cyber threats? Who decides which pieces of consumer information in their databases is deemed sensitive and how much protection it is afforded? To what extent is the security of their data subject to any minimum requirements or regulations and how does this differ from data held by other types of organizations? What should Congress be doing to mitigate cyber threats or to prompt dat brokers to do so themselves.

Today's hearing is an opportunity to think carefully about the oversight we ought to be providing from the kinds of information data brokers are allowed to compile and sell to the conditions under which that information is retained.

For my part, I believe Americans have a fundamental right to privacy. They deserve both transparency and

accountability from companies that trade on the details of their lives. And should they choose to leave personal information in the hands of those companies, they certainly deserve to know that their information is being safeguard to the greatest possible degree.

I hope this hearing will help us to identify the best ways to ensure the protection of Americans' personal information. I look forward to the testimony of our three witnesses and thank them for coming, and I thank you, Mr. Chairman.

[The prepared statement of Senator Franken appears in the appendix.]

Senator Flake. Thank you, Senator Franken.

Will the witnesses please stand to be sworn in?

[Witnesses sworn.]

Senator Flake. Let the record indicate all three witnesses answered in the affirmative.

I will introduce all three of you and then turn to your testimony.

Ms. Pamela Dixon is the Founder and Chief Executive of the World Policy Forum, a long-time commentator and researcher on privacy-related issues. She has authored important reports on data brokers and identify theft; a former research fellow with the Privacy Foundation at Denver University School of Law. She is also the author

of nine books, an expert advisor to the OECD on health data, and on the editorial board of the *Journal of Technology Science* at Harvard.

Mr. Justin Harvey is the Chief Security Officer at Fidelis CyberSecurity and has over 20 years of experience working at leading companies in cyber security and information technology. His primary security expertise is centered on the areas of targeted attacks, threat intelligence, security analytics, incident response, and security operations. Mr. Harvey has led incident response teams on several notable high profile breaches, including Sony in 2011, Foxconn in mainland China in 2012. He was previously CTO for Global Solutions at FireEye and chief solution strategist at Mandiant and Hewlett Packard.

Mr. Frank Caserta is the Chief Security Officer for Acxiom Corporation, one of the largest marketing, technology and services companies. He has been at Acxiom for over 20 years. He created and implemented the job he currently holds -- nice work if you can get it that way -- Acxiom's first chief security officer. At CSO, he has been responsible for global strategy covering information and physical security. Prior to his current role, he was Acxiom's Chief Technical Officer in the Services Division, where he transferred to Acxiom IT Data Center

in an industry-leading data warehousing technology and IT Center. Mr. Caserta also holds a number of certifications, including as a certified information systems security professional.

Now, all of the witnesses' testimony will be entered into the record in their entirety. I would encourage you to summarize your testimony to 5 minutes or less.

Thank you, all of you, for being here. We are really pleased with the panel today that we have assembled.

Ms. Dixon, go ahead.

TESTIMONY OF MS. PAM DIXON, EXECUTIVE DIRECTOR, WORLD PRIVACY FORUM, SAN DIEGO, CALIFORNIA

Ms. Dixon. Thank you. The World Privacy Forum calls on the Senate to pass minimum national security standards legislation. This is the largest remaining unregulated data store in the United States. It is time to close the gaps.

Senators, I have four points to make.

First, virtually nothing that data brokers have is unrelated to people in the United States. Literally, everyone has some piece of data attached to them in some way, shape or form. What data does not exist can be inferred. It creates an extraordinary network of information flows about ordinary consumers.

Let us be clear. The data we are talking about is my health data, it is your financial records, and it is your grandkids' genetics.

Second, it is reckless and downright dangerous to not protect this vast store of information. Minimum national data security standards would serve this purpose. It would allow data brokers to conduct their business, but it would keep Americans' data safe.

Third, let us be clear. This data that we are talking about is thoroughly unregulated. While entities

such as hospitals are covered entities under HIPAA, when a data broker stores the exact same information, unless they are a formal business associate of a health care provider, the same exact data is unregulated. This applies also in the financial sector, in the educational sector, and, of course, in the health sector, and even in the government sector.

Fourth, when legislation is passed regarding the security of information that data brokers held, it is going to be extraordinarily important to ,keep the legislation airtight and watertight. There should not be any exceptions that overcome the regulations.

One of the biggest areas is to try to define sensitive information. At this point in time, because of how data can be collated and analyzed, all data pieces end up having inferences and sensitivities. Therefore, it becomes incredibly important to ensure that all data is treated equally and is considered as sensitive.

Thank you for inviting me to talk with you today and I look forward to working with you on any forthcoming legislation.

[The prepared testimony of Ms. Dixon appears in the appendix.]

Senator Flake. Thank you, Ms. Dixon.

Mr. Harvey?

TESTIMONY OF MR. JUSTIN HARVEY, CHIEF SECURITY OFFICER, FIDELIS CYBERSECURITY, Bethesda, Maryland.

Mr. Harvey. Good afternoon, Chairman Flake and Ranking Member Franken. I am here to t5alk to you today about what are known as data brokers and the related cyber security challenges awe are now facing.

There are many legitimate and responsible ways to leverage sensitive information in this fashion, such as driving significant cost savings for consumers, health improvements and so on. But breaches and other misuse of data can cause great damage.

We need to harness the benefits of big data without opening the door to abuse. One major priority here is to strike the right balance between security and access. All organizations, not just big data brokers, struggle between locking down their sensitive data and making it available for use and analysis.

It is the age-old security problem. Too much security disrupts productivity and too little is too reckless.

Let us consider a case in point around encryption. As long as the personal information is not a credit card or something related to a person's health, there is usually not a business or legislative mandate to encrypt

the data. In fact, some companies see encryption as a headache since it slows down accessing the data and we have not seen widespread adoption of encryption to secure data while it is at rest and while it is being transported through the network.

Companies clearly need to embrace encryption as a minimum best practice. However, encryption is not a silver bullet. It is only one of many components in a strong information security program. In fact, the trust placed in encryption is sometimes misplaced.

Today's intruders steal legitimate credentials to access data. In other words, they access the data just like a legitimate system administrator would.

Ultimately, encryption is only as good as the weakest link in the larger data security ecosystem. Unfortunately, that weakest link is often the human factor, from clicking on a malicious link or opening up an unknown attachment to being tricked into giving up someone's password, like we saw with CIA Director John Brennan.

People still represent the largest vulnerability we have in cyber security. The cyber security field also happens to be suffering from a huge, epic information security skills shortage. A recent study found 30 percent of security jobs remain unfilled in America. I

think that programs like One Interrupt in Boston have the right idea by teaching high school kids -- high school-aged kids about cyber security is the right approach. Get them while they are young.

The adage I use when advising my customers is, quote, "Plan for the worst. If the information is stored online, it has a significant chance of getting leaked at some point or accessed by an unauthorized third party."

No data set is completely secure no matter how much security or encryption or legislation is placed upon it. We must face and prepare for the high chance that it will be stolen and possibly leaked. Sometimes the fallout is massive, as we have 21.5 million cyber attack victims in the Office of Personnel Management's database.

We also use another adage quite frequently, one from my previous CEO, Kevin Mandia, which reads, "Breaches are inevitable and when it happens to be big data brokers, the scope, scale and sophistication of sensitive data they possess make the stakes even higher."

The most obvious risk is widespread fraud. Should these data sets get leaked to the general public or sold to the highest bidder, this could have cascading effects on our economy. Imagine a breach where every American's name, Social Security number, address, email, phone number and mother's maiden name was leaked to the

Internet. The size of this data is not outside of the realm of possibility.

To put this into perspective, Ashley Madison, a Website for extramarital affair hookups, was breached. The incident had information on 36 million people and contained 10 gigabytes of stolen data.

Given that the last U.S. Census reported a little over 320 million Americans, a whole country's worth of personally identifiable information could, therefore, be compressed into 100 gigabytes. That is a little under twice the size of the computer game Battlefield 4, which our kids play, or ten seasons of *Saturday Night Live* in high def. Well, maybe seasons in Senator Franken's era.

But that amount of data could fit on a USB drive or this Apple phone. A breach of this size would have a lasting effect on the economy and national security as the government and corporations would rush to implement stopgap measures to respond to the leak. Consumers would also be harmed as they would essentially have to change every single password and reestablish their own secure place on the Internet. Identity recovery, in other words, could be as troubling as identify theft.

I am reminded of the famous caption from a 1993 *New Yorker* cartoon that has since become a maxim of the digital age. Quote, "On the Internet, nobody knows you

are a dog," end quote.

Well, in the aftermath of a massive breach, you may find that on Internet, nobody knows you are you. The information that big data brokers have collected and generated represents some of the richest meta data about citizens in the world. Meta data is that all important data about data that helps us understand the context and usability of the information we possess.

Unlike Internet surveillance which can be foiled by encryption in legislation, brokers have gotten their data firsthand from us as users.

The volume, detail and richness of information that bit data brokers possess make them a prime target for breaches, especially state-sponsored cyber espionage. Nation states likely see brokers as a one-stop-shop for intelligence on U.S. citizens. No need to breach 10, 50 or 100 other corporations in the U.S. when they could just go to one place or two data brokers and get all of the data.

What is worse is that they do not even need to steal the data. They can simply access it by compromising a data administrator's credentials.

Since I forgot my tin foil hat at home, I will not even begin to discuss the possibility of U.S. intelligence agencies using this meta data to find

threats.

Nation states that have access to threats meta data can easily track the habits of U.S. citizens for nefarious purposes. This could include shadowing a target of interest, say, a government employee, to discover online and real world habits in order to gain access to Internet accounts that have sensitive info.

Corporate boards must understand that the organizations that they oversee need to operate in a continuous response model by proactively hunting for breaches and implementing what we call Red Teams, which perform a sort of scrimmage safely against companies, playing the role of a would-be attacker.

A new study by HP Enterprise found that IT security spend is up 7 percent and that companies spend about 76 percent of their information security budget on blocking. Unfortunately, this is not working. Most, if not all, of the breaches that we have been seeing have -- these organizations have invested in preventative approaches, the blocking approaches, versus detection and response or a continuous response model.

Remember, it is not always about external threats or malware that you hear about in the news. Many breaches are perpetrated by insiders. I realize that my testimony today is probably drawing an uncomfortable picture of the

challenges we face. We need to accept the "when," not "if," reality that breaches will happen. Attackers can be relentless and clever, but so can we.

Fidelis is able to monitor the movement of data in real time and deploy sophisticated analytics to recognize immediately when a breach is taking place, follow the attacker's trail and freeze them in their tracks.

In closing, we are very much in the game and it takes commitment, ingenuity, and, I mentioned earlier, a move from prevention to a detection and response model. We are getting better and better at finding cyber attacks and so are the big data brokers. While we might not be able to stop all breaches, our ability to leverage big data for insights about these attacks means we are rarely in the dark and we are making progress all the time.

I know I went long. I appreciate your patience, and thank you, Senators. I look forward to questions on the matter.

[The prepared testimony of Mr. Harvey appears in the appendix.]

Senator Flake. Thank you for that very comforting testimony, Mr. Harvey.

Mr. Caserta?

TESTIMONY OF MR. FRANK CASERTA, CHIEF SECURITY OFFICER, ACXIOM CORPORATION, LITTLE ROCK, ARKANSAS

Mr. Caserta. Chairman Flake and Ranking Member Franken, it is my pleasure to represent Acxiom at today's proceedings.

Acxiom has two main lines of business. We process our client's' information on their behalf, both ensuring its accuracy and analyzing it to help them find new ways to service customers.

We help our clients successfully manage audiences that they wish to reach and connect with these audiences. Through our services, our client are able to personalize their brand experiences for their customer and crate relationships that benefit both the customers and the brand.

The second line of our business is information products and services, what you would call being a data broker. These are primarily for fraud detection and prevention and fo marketing.

At Acxiom, we start with privacy. The Acxiom privacy program is built on the ethical use of data, ensuring that the use of data products and services we provide to our clients is legal, just and fair for all stakeholders, including the consumer.

Our program includes the credentialing of clients to ensure we are working with good actors and with legitimate interests, who themselves are accountable for the appropriate and ethical use of our products and services.

Importantly, we have an obligation to secure both the data in our data products, our services, and our clients' data that we are stewarding, the supplies to Acxiom's access to data or clients' access to their own data and prevention of unauthorized access and use of that data by anyone else.

Regarding security, our business is data-centered. So perhaps more intensely than others, Acxiom understandings we have an inherent responsibility to safeguard personal information we process for our clients and information we bring to the market. We work within our industry and across the commercial spectrum and with Federal, State and international governments to develop and implement best practices for data collection, use and protection.

A strong commitment to privacy and security is a core component for our brand. Like consumer-facing companies, data companies are subject to regulation by the Federal Trade Commission and are required to employ reasonable security measures to protect systems and information.

Each company decides what constitutes reasonable security base on the unique threats they face.

The resulting plans companies develop are necessarily confidential to protect company security. We are happy to characterize the general parameters of Acxiom's security program. However, we cannot provide so many details that we compromise our security. Further, we are not in a position to comment on other companies' internal confidential security measures.

Broadly speaking, our security program is designed to exceed Federal requirements for safeguarding data. We are often the leader in adopting new security techniques and protocols for the protection of data. For example, even though Acxiom's marketing information products are not covered by the Gramm-Leach-Bliley Act, we nevertheless apply the GLBA safeguard rule to those products.

Ultimately, Acxiom's approach to information security goes beyond what is required by either the law or self-regulation. That is, in fact, for Acxiom, a brand trust essential.

As our economy is increasingly data driven, Acxiom faces the same challenges all public and private sector operations have when using data. New technologies and data uses bring amazing opportunities to consumers,

business and governments, but with that come rising threats from criminals, activists, state-sponsored espionage, and others who want to exploit the technology and data for their own purposes.

It takes constant vigilance and investment to stay ahead of security challenges. The comprehensive security policies governing a company's operations must be backed with effective governance that will assure adequate protective measures are taken.

Good governance models include executives focused on security, risk management, privacy and audit; use of modern security control frameworks, like ISO-27000, and in the cyber security framework; audit programs for independent inspection and reporting covering security effectiveness; well executed security programs, monitoring, and instant response capabilities.

I have expanded on this topic in the written testimony submitted by Acxiom. I look forward to your questions and hope we can assist you in your mission today.

Thank you.

[The prepared testimony of Mr. Caserta appears in the appendix.]

Senator Flake. Thank you, Frank. Thank you all.

Ms. Dixon, you stated in your testimony right in the

beginning that there is basically nothing off-limits in this world.

Can you give some sense of some information that is held by data brokers that many Americans might be surprised that they have given out or that they have?

Ms. Dixon. Intriguingly enough, the data actually covers almost all areas. So health, finances -- let us just take some examples from that.

Many Americans do not realize that if they have made an over-the-counter purchase, they may well have what is called an inferred disease, that they actually end up on a list with that inferred disease, diabetes, heart disease, cancer even, HIV-positive status, based on the things you buy and some of your activities.

The other thing that is frequently on data broker lists or in their data stores is a lot of financial and what I would call ownership information, the make and model of the car you own, how many children you have, the ages of your children, whether or not you graduated high school, college or graduate school, whether you rent or own a home, what is your exact income, do you owe money to the Federal Government, do you have a tax lien.

All of this data is quite commonly held by data brokers. In some contexts, this data is actually regulated, particularly data about debt, if you are 30,

60 or 90 days late on a mortgage, for example. But when it is held by data brokers out of these contexts, then it becomes unregulated and the GLBA, HIPAA and other Federal protections for this data evaporate.

Senator Flake. Let us turn to one of the breaches. Recently, October 1, it was revealed that Experian, one of the biggest data brokers, experienced a large-scale breach in the credit reporting arm. I think 15 million people had their personal information stolen by hackers, including names, addresses, Social Security numbers, birthdays, perhaps even drivers' licenses, military IDs, and passport numbers.

It has been reported that according to ex-Experian sources, Experian had been suffering from a corporate culture that failed to take security seriously. One former employee said, "Once the leadership changed, the focus changed to controlling costs and not even taking systems down for maintenance and investments started disappearing from a lot of areas. We were in the middle of putting into operation certain tools to do next generation detection of cyber threats, but we were not able to get many of them into production. That is how Experian wound up being where they are now," unquote.

Ms. Dixon, do you think this is true about Experian? Is this just a culture that develops over time, that you

do not take security seriously?

Ms. Dixon. I cannot speak to their internal culture, but what I can speak to is the really disturbing data breaches that they have had that have continued.

There was a case where there was a previous Experian breach where data was literally sold to entities under investigation by the Department of Justice. They then committed fraud and then real people, just people, lost their homes as a result.

This was a major FTC and DOJ investigation and we have additional new breaches. So it is difficult to say what is going on inside, but that does give me a real indication that something is wrong.

Look, in order to have a fix for this kind of a cultural problem and a technical problem, we do not need to reinvent the wheel here. There are already good use models in place. The HIPAA security rule provides a highly complex sector with adaptable and flexible minimum national security safeguards that have been implementable and helpful. And we have NIST standards already in place and an agency ready to create standards.

We have CFPB for larger participants and we have the FTC for smaller players. We have got the tools that we need to create these minimum requirements. And if we had examinations of companies on national security

requirements or security standard requirements, I think it would go far to correcting that kind of lax behavior.

Senator Flake. Mr. Harvey, what security measures would have been -- could have been adequate for the sort of operation that Experian had? Would something like the HIPAA model, something that had been applied, would that have prevented it?

Mr. Harvey. No. No. You see it across the board. PCI, the payment card industry, data security standards, which is known as DSS, the HIPAA standards, these types of standards are -- give organizations a low bar to aspire to. It is the bare minimum and all of these standards were written 5 to 10 to 15 years ago when there were no state-sponsored espionage against -- being conducted against corporations in America.

Take, for instance, the Anthem breach. They were HIPAA-compliant, but they still lost all of their records. And what is necessary is to focus on a few points like mandatory encryption for all private data, and we can -- we can go to the experts on what private or sensitive data is.

Moving from a prevention model to detect and respond, there is a gap here where -- we call it the dwell time, from when there is an attack and when you discover it.

Do you know what the average is last year -- 205

days. That means, on average, an attacker could be in an organization for seven months without being detected. We have to get that down to days, if not hours, if not minutes.

And then, finally, there is just simply not enough people out there, not enough trained cyber security workers in any market, let alone the large ones. Consider the smaller towns that have large corporate headquarters, it is very difficult to hire and retain skilled cyber security talent here.

So what is needed is a higher bar, something that really focuses on being more data-centric versus legislation or laws or standards that are 10 to 15 years old.

NIST does not address the privacy of the data. The Federal Government uses NIST, but it is still getting breached. So we need to -- we need to think about how we change the game. And, finally, it is not CIS-SA. It is not threat intel sharing. Threat intelligence is only as good as the last person it was affected by.

A lot of the attacks that are being perpetrated today are what is known as zero day or their signature list, which means they have never been -- they have never been seen before. So in those cases, sharing threat intel with the government would not have helped.

Senator Flake. My time is up.

Senator Franken?

Senator Franken. Thank you, Mr. Chairman. I have the feeling that Fidelis has a detection and response model. That is what I kind of got out of your testimony.

Mr. Harvey. A little bit. But I would also say that it is not --

Senator Franken. Let me ask a question first.

[Laughter]

Senator Franken. You have had your time.

Ms. Dixon, am I hearing any disagreement here between you and Mr. Harvey? There is a difference between oversight of what we have to do. You were talking about perhaps the CFPB or the FTC establishing oversight.

How does that play into the kind of security that Mr. Harvey is talking about? Put both of your testimony together for me, would you?

Ms. Dixon. Absolutely, and thank you.

Senator Franken. For your responses.

Ms. Dixon. I still like the idea of a minimum national security standard for data brokers. We have to start somewhere. We have to start in a place where we do not have to stand up a new Federal agency and we have got to work with the tools that are on hand.

The HIPAA security rule, if you can imagine a world

without that rule, I do not want to personally. I mean, we already have data breaches, but I believe we would have had many, many more. It does have and does provide a measure of accountability and effectiveness and I think it is an important starting point.

Now, I agree that these rules were written at an earlier time. However, they are adaptable, they are flexible, and updatable, and this is exactly the kind of technology-neutral standard that we need so that we do not bring business to a screeching halt, but that we also, at the same time, provide protection and some risk -- help for Americans who have their data stored, typically without their knowledge, at these companies and these decisions that the data is used for can really impact their lives.

So I really like the idea of a minimum standard. It can be a floor, not a ceiling, and let us start there.

Senator Franken. Well, let us say the Senate and the House were legislating bodies. How should Congress address this?

Ms. Dixon. Legislation would be a great first step addressing the issue of what data is collected, where it is stored, how it is stored, looking at the privacy and security safeguards, all of the baseline things that we already see in models, like the HIPAA security rule and

even the safeguards rule in GLBA and even some of the rules in FERPA. There are a lot of models to pull from.

Senator Franken. In the meantime, what steps could the Executive Branch take under its existing authorities to protect Americans' personal information?

Ms. Dixon. I think the existing authority that we have right now would fall under FTC Act Section 5, Unfair and Deceptive Business Practices. I think that would be a good start.

I like that Acxiom is, in a voluntary way, holding their marketing data under GLBA. That gives consumers the opportunity to opt out. If this could become a best practice across the industry, that would be fantastic.

I would like to note that to its credit, Acxiom created the "About the Data Portal." I have noticed that not one single other data broker in the industry of thousands of data brokers has anything similar that allows us to see our data and then opt out.

I am not saying that Acxiom is perfect, I am not going to give you that free pass. However, that is an important first step.

Senator Franken. I think that is why Acxiom is here, because of that.

Ms. Dixon. Right. But, look, that is an important first step and we should not minimize that important

step. That is certainly a good place to start.

Senator Franken. And thank you, Mr. Caserta, for being here.

Mr. Harvey, you have spoken about the inadequacy of focusing on threat intelligence sharing and need for other measures. You have sort of laid out what you think would best protect us, which is a detection and response model.

Do you think it would be possible for the Federal Government to impose effective minimum baseline data security standards would improve the security of data brokers?

Mr. Caserta, you can certainly feel free to answer this, as well.

Mr. Harvey. I believe so. I think that the -- Ms. Dixon did a great job in discussing the need for minimum requirements.

The one thing that I did not hear you mention is the EU's GDPR, the General Data Protection Regulation, which is to be instituted in 2018.

Now, I am not a big fan and following everything that the Europeans do, but in this, I think that it specifies into much greater detail the handling of private data, breach notification timeline, which is really important since in the U.S. breach notification laws and

regulations differ from state to state. It would be helpful to have one single standard across the board and I do believe there is a way for the Legislative Branch to recommend --

Senator Franken. Senator Leahy has a breach notification bill that includes that.

Mr. Harvey. Correct. But for the technical aspect, yes, to be able to recommend and require companies -- and it is not just Mr. Caserta's firm or the data brokers. I believe that if an organization, regardless of commercial, government, defense, whatever, has private or sensitive data, then they should be -- they should fall under the same guidelines.

Mr. Caserta. I would iterate that, as well. We have been supporting a move towards breach notification laws for about 10 years and they have stalled out for a variety of reasons in the legislative bodies over the years. But it would be helpful because it is very distracting and challenging to figure out how to navigate all that and to know when you are right or wrong.

As to the overall regulation, you know, with the FTC and the other rules, it is interesting. Our client base also has a fair amount of regulations in the financial services industry and things like that. They apply those rules to us. Even if the direct regulating authority

does not, since they are accountable for the business that they do with us, they extend those same rules and they audit us to those rules. So we are indirectly regulated that way, as well.

So for large companies, you know, regulated companies, those rules are being applied. That regulation is extending out into the third parties quite a bit.

Senator Franken. Thank you. Thank you for letting me go a little over, your indulgence.

Senator Flake. You bet. Senator Blumenthal?

Senator Blumenthal. Thanks, Mr. Chairman.

Thank you all for being here today. Over the years, I have worked to reform this area where consumers can be so much at risk of abuse and privacy invasion and I will be introducing the Do Not Track Online Act, which would give consumers a way to indicate that they essentially wish to block their personal information from being collected by providers of online services.

Unlike the voluntary efforts that industry has promised from time to time, but never really delivered, my legislation would give consumers recourse and remedy if their privacy preferences are ignored. This bill is essentially the same bill that Senator Rockefeller and I introduced during the previous session. It would provide

real rights and a means to enforce them against the abuses and overreach and intrusive practices that have become all too common, indeed endemic, to much of this industry.

Ms. Dixon, I think essentially I know the answer to this question, but you would support that kind of legislation.

Ms. Dixon. Yes. Of course, I would like to see it and I look forward to reading it and working with you on it. I think it is incredibly important to attack this problem from a multiplicity of angles and at a lot of different layers.

So, yes, I would support that legislation.

Senator Blumenthal. The bill would provide very limited exceptions, but would prohibit online providers from collecting personal information from individuals who indicate such a preference.

I take it from your testimony that you would reject the notion that the market or competition among individuals in the industry is sufficient to protect consumers.

Ms. Dixon. I am afraid that I am not able to say that that is happening correctly, as it should. We have a lack of balance right now in the market that has not been sufficient to correct that problem.

Senator Blumenthal. In your testimony, you point out that context is very important to assessing whether a particular piece of information is sensitive or not. A lot of Americans, for example, feel that their home address is not sensitive information.

Ms. Dixon. Yes.

Senator Blumenthal. But an American and most especially a woman who has been stalked or abused or has fled a situation of abuse may feel very strongly, and understandably, that a home address is, in fact, sensitive information.

If a consumer decides that her personal information is sensitive and should not be bought or sold by data brokers, can she stop her information from being and sold right now?

Ms. Dixon. Not right now. And I agree with you completely about how information is contextual. That is what makes this issue so tremendously challenging. I became incredibly sensitized to the issue of home address through my work with the National Network to End Domestic Violence and women who you would think, okay, home address, no problem, email address, no problem, but for them it was a life-threatening situation. So this did sensitize me as to how even information that is deemed public information can be a safety threat. And it

becomes complex to solve that problem.

So the opt-out that allows a person to decide when they have a problem is incredibly important to accomplish. So, yes, I agree. I think that is a good solution.

Senator Blumenthal. In fact, the Senate Commerce Committee, where I also sit, conducted an in-depth inquiry into the practices of nine major data brokers and in response to the committee's questions, we found some companies actually sell profiles that define consumers in categories or score them without the consumer's permission, often without their knowledge.

Those categories included, quote, "rural and barely making it," end quote, or, quote, "ethnic, second city strugglers," end quote, or, quote, "retiring on empty," end quote.

My belief is that consumers themselves are in the best position, most knowledgeable and best equipped to decide whether a particular piece of information is sensitive to that consumer herself. Would you agree?

Ms. Dixon. I agree, absolutely, and you are absolutely correct. In an era of big data, data -- the pieces of information that data brokers have about us do not just sit there. They can be combined to create new data and new inferences, and that is what creates those

categorizations. And I worry about a world in which people are categorized in ways that they are not aware of and I would like to see people aware of these categorizations and given real choice about what happens to them based on those.

Senator Blumenthal. Well, this legislation would require clear, unequivocal notice to the consumer about the collection and use of that information and would require affirmative consent to that use. In other words, essentially, consent, knowledgeable, fact-driven by the consumer based on his or her situation.

You are absolutely right. We live in an era of big data; in fact, an era of bigger and bigger data, which makes the consumer sometimes smaller and smaller in her ability to control how that information is used.

So I think this legislation ought to gain momentum and hopefully the very informational hearing that we hare having today will help drive that momentum. Thank you.

Thanks, Mr. Chairman.

Senator Flake. Thank you.

Senator Whitehouse?

Senator Whitehouse. Thank you, Chairman. I have just arrived. I was on the floor with a colleague who invited me to his maiden speech. So I wanted to show him the courtesy of attending.

But I appreciate this very much and I appreciate your attention on the privacy concerns that all this data being out there creates. I think there is at least a thread of thought that if it is the government that is collecting data of any kind, then there are dramatic immediate harms that occur virtually from that fact. But if it is the private sector collecting data, almost no amount of intrusion into your electronic profile, into your emails, into your conversations, into where you go and when you are there and all of that is a problem.

I wonder if I could just ask each of you, as we wrap up, to speak about what you see as the most significant privacy dangers that would could from a pure private sector misuse of this sort of big data for a regular individual.

Let me start with Ms. Dixon and go right across to Mr. Harvey and Mr. Caserta.

Ms. Dixon. Thank you. The thing I worry about the most with this is data that is layered. So, for example, census data that includes your zip code layered with other financial and lifestyle data that is then used to determine the kinds of offers that you see, for example, for credit, for educational opportunities, and even for job opportunities.

That is what worries me because this puts people,

based on their zip code and other factors about themselves, that they cannot change. It puts them into a bubble that is not necessarily of their own making, and, to me, that is just plain un-American. I still believe in the American dream and I would like to see data help us achieve our dreams, not hinder them.

So that is the thing I worry the most about. So I would like to see legislation that provides minimum security standards for data brokers so we have less risk of that data being subject to fraudulent use and criminal abuse. But I would also like to see the ability for all of us to have the right to shape our digital exhaust that we have just from living our daily lives.

Mr. Harvey. Good afternoon, Senator.

I have broken it down into a few areas. The first is just the inability to correct the data.

Senator Whitehouse. I only have about a minute given the time we are working under.

Mr. Harvey. I will be brief. The inability to correct the data once it is out there with these big data stores, it is very difficult to unwind given the way that big data analytics operates.

The second one would, of course, be the right to be forgotten.

On a larger scale, I am concerned with there being a

big breach where all of our personal data is out in the open and instead of an attacker selling it, an attacker would leak it to the Internet. We saw them do that with Ashley Madison.

If were to do -- if someone were to do that with our personal data, let us just say all of our name, address, Social Security number and phone numbers and email addresses, they could essentially reset all of our passwords. They could wreak havoc on every single online service trying to impersonate us.

Then, finally, it is the state-sponsored aspect of this. Like I had mentioned earlier, if an attacker were to get access to this data, a nation state-sponsored -- think cyber espionage or cyber terrorism, they would have basically a treasure trove of data to mine and to look through in order to abuse in a multitude of ways.

Senator Whitehouse. Finally, Mr. Caserta?

Mr. Caserta. Thank you. So we have a privacy practice that focuses a lot on that element. They would probably go into a lot better detail on the ethical use of that data and we spend a lot of time working on those issues.

From my perspective in the security world, it is the data breach aspects. Those are the things that I worry about the most. It is where I spend most of my time,

looking at the challenges with the technical aspects that a lot of companies are operating with, the Internet and privacy challenges that come with that; looking at how to source the individual technical skills in people to work on these challenges. It seems like the bad guys can grow them faster than the good guys can at times.

So those are some of the more pragmatic things that I am worried about day-to-day on the security side, but we couple that 100 percent in that privacy context.

Senator Whitehouse. Thank you.

Senator Flake. Thank you.

Let me follow on. My last round of questions had to do with Experian and that data breach there.

Mr. Caserta, I did not have time to get to you. To the extent that that was kind of the corporate culture described by an ex-employee, is that endemic of data brokers?

Mr. Caserta. I certainly hope not.

Senator Flake. How is your company different?

Mr. Caserta. I certainly hope that is not endemic, but the cultural aspect is something we tackled head on many years ago because ultimately, as a data company, we have a lot of people that work with data and the better trained they are, the more aware they are in understanding how to apply appropriate security, how to

apply encryption, how to be aware of phishing attacks and other sorts of intrusions that come into the corporate world, the more effective our security program would be.

So we invest in quite a bit of training. We have mandatory security and privacy training for all associates in our company and I get the luxury of revoking their access from our network if they do not complete that training. So that is an interesting combination sometimes.

But the idea is to put it in an enterprise risk framework and make sure that we are having an executive and board dialogue around real risks; what is substantive; what are we dealing with; where do we need investments. And it is not just security. It is upgrade aging systems. It is a culture of evergreening and moving forward to make sure that you can maintain a decent security posture.

Senator Flake. Let us turn to the OPM hack. It is increasingly clear that our strategic competitors have an interest in that. That was a lot of government data and security data with regard to intelligence, officials in our intelligence business.

Is there a threat -- Mr. Harvey, you seem to think so -- from our strategic competitors or other nation states to hack this data. If so, can they not just buy it?

Mr. Harvey. It is certainly possible that they could buy access in legitimate ways through proxy groups. Just like we have seen suspected Russian state-sponsored espionage operating through proxy groups in Eastern Europe, I am sure that our close allies, sarcastically, could both do the same. But it is absolutely a danger for this data to be accessed by or leaked to nations that want to conduct espionage operations against the U.S.

Like I said before, it is easy for them to -- it is like the 7-11 of data. Go to a data broker, hit them up or get access to a data administrator's console, access the data rather than go hit 10, 20, 30, 40 other organizations.

Senator Flake. Mr. Caserta, is there a difference between the data available for purchase from a data broker and that that is held by the data broker?

Mr. Caserta. Yes, there are differences. We have marketing data elements that are very generic in terms of categorizing and looking at buying patterns, things like that. There is also basically identity data that is used as -- we call it reference data and it is used to specifically do things in the identity verification world. That data is much more granular and it is extremely restricted in how it can be used.

The use cases around that data and how we let

somebody have access to something like that is very intense, very limited, a very small part of our business. The marketing data is quite a bit larger in terms of the data broker side of what we do.

The our hosting services, we are managing a lot of data types for a lot of companies that come through for the integration services and enhancement work that we do for them.

So we end up using a pretty high bar for security across all three categories of data, because from a security perspective, none of them are less important than the others in terms of trust with our clients.

Senator Flake. The question was asked of Ms. Dixon if legislation were being written, what form should it take. Let me ask you. In terms of legitimate business and making consumers' lives easier and everything else, where should we tread lightly here and what should we be concerned about and where can industry act on its own to police itself?

Mr. Caserta. I know our privacy group spends a lot of time on that topic in terms of the beneficial use of data and so forth. I do think that data breach notification and other things like that could be helpful and it is one of those areas in looking at because it confuses consumers when they get so much notification for

so many things.

The tendency today is really to over-notify just to be extra careful when you incur a situation, whether there is a harm trigger or not. So there are a lot of things that go into that kind of legislation. But I know from the security perspective, the breach notification areas are something that definitely needs some retooling.

Senator Flake. So some kind of uniform standard there among the industry.

Mr. Caserta. Yes. Preempt all this different state legislation and everything that we are dealing with.

Senator Flake. Thank you.

Senator Franken?

Senator Franken. Thank you. That is interesting, unless maybe the state is tougher.

Mr. Caserta, when you tell people you work for Acxiom, do they have any idea what it is you do?

Mr. Caserta. Generally not. I mean, it is definitely a power behind the brands. Right. You know, we tend to be the processing behind a lot of other brands to help them do what they need to do.

Senator Franken. Sure.

Mr. Caserta. But we have stepped out a little more recently on that front.

Senator Franken. Well, it is just that I think

people are not aware of what information is being taken about them. Is that not fair to say?

Mr. Caserta. I think it is fair to say. It is one of the reasons we did Aboutthedata.com. It was a way to get people a chance to look at some of that data and get an idea what it is we do have and what a data broker can do, and I think that is helpful and I think we could see more of that.

Senator Franken. Is that the Website where consumers can see information that has been collected about them?

Mr. Caserta. Yes. The information that we have collected them.

Senator Franken. And they can opt out of certain marketing programs.

Mr. Caserta. Yes.

Senator Franken. Okay.

Mr. Caserta. Yes.

Senator Franken. But many of your competitors do not offer that, right?

Mr. Caserta. As far as I know, they do not.

Senator Franken. Right. And there is certainly no uniform law requiring that kind of basic transparency and accountability.

Mr. Caserta. No.

Senator Franken. Well, that is why I am a cosponsor of Senator Blumenthal's Data Broker Accountability and Transparency Act -- I think Senator Markey is now. It was Senator Rockefeller's -- which would address that gap and give -- because I do think that people have a right to know what is being taken and to give permission.

Do you think it is time that all companies did what your company is doing?

Mr. Caserta. I probably do not know that I could speak for all companies like that, but we thought enough about it to do it.

Senator Franken. Okay. I will take that as an answer. No, it is not. My goodness. You could speak it as yourself as an individual, can you not?

Mr. Caserta. So it is hard to separate yourself from the company.

Senator Franken. Never mind. I am sorry. You have got to go to the conferences. I understand.

My understanding is that today, even when a consumer is given the chance to opt out of certain marketing programs, that your company, a company like Acxiom may stop selling the information for marketing purposes, but may still keep the information in its databases, where it remains at risk for being in a data breach.

Is that your understanding, as well?

Mr. Caserta. In a limited fashion, yes. We do clean out data on a periodic basis. Obviously, a key security strategy is to limit the footprint of how much data you have over time. We are much more interested in keeping current data and not necessarily keeping years and years of stale data, which just can represent a risk.

Senator Franken. Now, do I understand from your testimony that some data is considered very personal and very sensitive data, but I do not think there are legal definitions for that. Are there, Ms. Dixon?

Ms. Dixon. There is not a consistent legal definition of what constitutes sensitive information. There is one for Europe, there is one for various sectors, and then there is a variety of self-regulatory definitions.

Senator Franken. Mr. Harvey seems to be a big fan of Europe. Am I right?

Mr. Harvey. I like French food once in a while.

Senator Franken. But I mean they have -- do they do this in a better way, define this in a better way than we do?

Mr. Harvey. I have not looked at the legislation enough to comment on that.

Senator Franken. How do you decide within Acxiom which is particularly private and sensitive information

and which is not?

Mr. Caserta. So our privacy group goes through a lot of the legislation. A lot of the governing bodies for marketers, they do this globally and they synthesize out for us a list of data that they consider to be sensitive or restricted and they apply those rules to every data product and every data service that we provide.

So we are trying to set the bar high and understand where that goes. They also look at what they call the creep factor. Is it something that is just not even appropriate for consumers regardless of its regulatory nature? And they apply those rules to the company.

Senator Franken. Ms. Dixon, what is your understanding of how data brokers decide what is and what is not sensitive information and what should we be doing to harmonize this across the industry?

Ms. Dixon. This is a difficult issue because sensitivity is defined contextually by both consumers and by companies. So in my written testimony, I have listed three different definitions of sensitive data. One is Acxiom's definition in one of its B-to-B contracts and the other one is from the Network Advertising Initiative and one is from the DAA. Both are self-regulatory kind of ad network, self-regulatory programs.

And in all of those definitions, it is so frustrating because medical data is defined in a very focused, narrow way. And right now we know that health data is becoming defined more broadly with Fitbits and Apple watches and health data being gathered and collected outside of the constraints of HIPAA.

So the very narrow definitions of, for example, a medical diagnosis is sensitive data compared with, oh, well, maybe genetic information is sensitive data. Basically, what ends up happening is that each company then ends up, and through no fault of its own, but they use their own filters to determine what constitutes sensitive and no one agrees on what this is. That is a problem.

Senator Franken. Yes. That is an issue for us to contend with.

Thank you again for your indulgence, Mr. Chairman.

Senator Flake. Thank you.

Senator Tillis?

Senator Tillis. Thank you, Mr. Chairman. I am sorry I am late. One of my freshman colleagues gave his maiden speech today, very patient. He waited a year actually to do it. That is remarkable.

Senator Franken. How was it?

Senator Tillis. It was great. It was actually the

best.

Thank you all for being here today. I want to start with either Mr. Harvey or Mr. Caserta. I worked in a data analytic practice. I worked in two different industries that used the information to know more about the customer and then kind of use that information to be instructive in terms of the customer experience and giving the customers more value.

So I think there is a lot of positive that can come from the use of this information. The real question is how do you manage abuses and then how do you protect the risk, privacy, a number of other factors.

But when you have this problem come up, I have never seen government -- never saw a problem that government did not want to over-regulate and I think that there is a big risk that some of the upsides, some of the positive aspects of using this data could be at risk if we react and come up with a government solution before industry has been able to come up with their own sorts of standards.

Can you give me some sense about where we are in the industry and what things we could look to to address some of the concerns with respect to exploitation or with respect to privacy concerns, having the customer have maybe some right or vehicle for opting out if they choose

not to have their information brought into the fold and the benefits or risks of having that consideration?

We will start with you, Mr. Caserta.

Mr. Caserta. Okay. There were a number of angles in that. I want to try to cover some of that. So from a privacy perspective, it is maintaining an understanding of what is appropriate use of that data, and then from a security perspective, looking to detect fraudulent use of that data.

So somebody may have a perfectly legitimate reason to look at something, but then you start to look at how they are using the data, the access patterns around the data, and you ask the question is that legitimate.

We have to do that with some of our more sensitive risk data products, where we actually monitor the type of inquiries that come in on that data for inappropriate access. Doing that at scale I think has some technical challenges, but I think it is one of the directions in the future that we would be doing more of and I think that would be a serious consideration over time, how to put fraud detection on top of data use.

Senator Tillis. Are you going to be able to keep up with the pace? It is a big order, because you are providing access to enormous sums of data in real time with billions or potentially trillions of transactions.

So how are you going to stay ahead of the curve and convince us that the industry can deal with the potential exploitation?

Mr. Caserta. I think setting the self-regulation out there in the work that we do is helpful. Again, I look at the nature of breach notification, how hard it is to get out, what type of data breach, what was the impact, where did it come from, because a lot of the security industry learns from the mistakes of what has occurred, tends to try and close gaps.

The hard part is to predict what has not happened yet. Some of the intelligence discussions that are going on out there have potential to help with some of that, but it is very challenging to make it useful.

So I do think that the risk management practice of understanding the risk with the data, putting a proper governance process in place to understand that you are going to time your investments with that data, that you are going to upscale your security, you are going to upscale your infrastructure and make sure that all of your security program is kept in line with that data is a critical aspect that has to occur.

Senator Tillis. Mr. Harvey, similar line of questions. I know we have covered a lot of ground there. So you can pick and choose. With the time I have

remaining, Mr. Chair.

Mr. Harvey. Well, coming from a vendor doing cyber security, I think we kind of look at this in a couple of ways, a choose your own adventure.

One would be for big data brokers to do self-regulation, like the payment card industry or high trust with health care. There are pros and cons. No one know -- if you take that approach, no one knows their data better than they do, but the on the con, you have them policing themselves.

Then there is the legislative or the law angle for you, being the Legislative Branch, to put out. The pros of that would be that it could apply to all corporations. I think we are missing sight here that we are talking about these big data brokers that have terabytes and pedabytes of information, but, gees, go look at any Silicon Valley company and they have almost as -- Facebook, Google, they all have huge amounts, vast data stores of very sensitive data.

So if Congress is going to act on this, expand the scope and talk about minimum standards for the privacy of data, define what private data and sensitive data is, and, if I can give some advice here, set the bar pretty high, because we do not want legislation or self-regulation to be the minimum that organizations aspire to

and then they think, "Oh, I am compliant" and then they can just kind of, "Oh, I am not going to fund anything above that bar" and we really do not want to see that in the industry.

Senator Tillis. Ms. Dixon -- just very briefly, Mr. Chair, if I may -- what kinds of regulatory constructs make sense? We are talking about the spectrum of self-regulation to potentially overreach on the part of the government, which takes us away from some of the very positive aspects that come from responsible use of this information.

What does a right size regulatory framework look like?

Ms. Dixon. Right. I agree with you on that, that we want good data uses and we want to curtail the harmful uses or the data abuses.

I have thought about this a lot and I keep coming to the HIPAA rule. I do like how the HIPAA rule tamed an incredibly complex sector with flexible regulations that apply to a huge scope of company size and business structure.

The data broker industry is quite complex. There are many, many permutations and types of businesses. Acxiom is a large multinational business. But there are also 2 percent mom-and-pops. So we are going to have to have

something quite scalable.

I like the idea of minimum security regulations and standards for data brokers because, first, the larger participants are going to have different capacities than the smaller participants, but the smaller participants will be helped and they will have a clear idea of what is expected of them and what are the minimum necessary standards.

In terms of self-regulation, that is a good question. Of course, we all hold out hope for self-regulation, but as I mentioned earlier, in the data broker sector, Acxiom is the only company that stepped forward and did any kind of anything having to do with self-regulation. The rest of the industry has not come along and it has been 2 years. They have had ample opportunity and they did not take up the bar.

Therefore, I think we have given them a fair shake and I would like to see some -- especially in the area of security, I would like to see some standards. Keep the data safe.

Senator Tillis. Thank you. Thank you, Mr. Chair.

Senator Flake. Thank you. I believe a vote has been called, but we still have quite a few minutes. Go ahead.

Senator Blumenthal. I just have a couple of quick

questions. In the bill that I am going to offer, State Attorneys General, along with the FTC, would have enforcement powers, but the State Attorneys General would have to yield if there were a pending Federal action.

I wonder, Ms. Dixon, if that seems to you like a plausible way and good way to enforce this law.

Ms. Dixon. I really liked how that bill was constructed in regards to enforcement with the State AGs. If you have an extremely active State AG with feet on the ground and they see a harm right there, I really like the idea of the State AG being empowered to work on that. And I would imagine that there would be a collegial relationship between the enforcement bodies and that could all be worked out.

Senator Blumenthal. That answer certainly confirms my own experience as a former State Attorney General, that there is a collegial relationship and that, in fact, the areas of interest and objectives are very much consistent and in alignment.

Mr. Caserta, I recognize that your company was one of the first to come forward with some standards. At the same time, I must say that the Senate Commerce Committee, as you will recall, in 2013, conducted an inquiry into how the data broker industry operates, with specific focus on those nine companies, I mentioned them earlier,

that sell consumer data for marketing purposes.

The report, as you may also recall, said, quote, "While some of the companies have been completely responsive to this inquiry, several major data brokers to date have remained intent on keeping key aspects of their operations secret from both the committee and the general public," end quote.

Acxiom was cited as one of those companies. Quote, "Three of the largest companies, Acxiom, Experian and Epsilon, to date have been similarly secretive with the committee with respect to their practices, refusing to identify the specific sources of their data or the customers who purchase it."

I would like to ask you whether you can commit, on behalf of your company, that you will share the specific sources of Acxiom's consumer data and the customers to whom you sell it with this Committee. I do not know that we and our constituents can trust data brokers if they operate completely behind a veil of secrecy and I make this point to you because your company has been more at the forefront of this effort than lagging behind it.

So it may be unfair to you because you are the one here, which I commend you for being, but I feel compelled to ask you this question.

Mr. Caserta. Yes, sir. I cannot make that

commitment direct up today. I would say that it is -- to have more dialogue on it, to come back and visit that. A lot of the -- as I understand it, because I was not part of that discussion, but a lot of extremely proprietary, extremely sensitive questions were being asked that is very dangerous to disclose, not from a consumer perspective, but from a competitive operations perspective and maintaining our ability to operate with our intellectual property.

So I want to be very careful with that, but I do not ever want to exclude the need to have the dialogue and to continue to have the dialogue.

Senator Blumenthal. I would like to have the dialogue. I respect that there may be proprietary interests at stake. I am not aware of how they might impact, for example, the sources of information. I can understand maybe consumers or customers rather. But I would like to continue discussing it.

Thank you. Thanks, Mr. Chairman.

Senator Flake. Thank you. We have time for two. We have only had one round. Do you have one question for a minute?

Senator Franken. Yes. I just have one question for everybody. This is kind of a factual question. But I am wondering how these requests come in and if there is a

way to make sure that the requests come in in a certain way.

So if somebody wants to day I would like to find all of the evangelical Audi-owning skiers who live west of the Mississippi, that is one thing. If they want to say there is this guy named Justin Harvey and I want to know everything you know about him, that is another thing.

Do you have a filter for what questions you allow people to query your data with?

Mr. Caserta. Yes, sir, we do. So we go through a basically use case analysis, what kind of a client is it. Somebody that is going to ask a specific about an individual question, that is a very limited, very narrow permissible use for our risk product, collected only for that use and extremely limited and credentialed as to who can do that.

The general marketing questions tend to be much broader where they are not targeting an individual. They are looking for behaviors and/trying to generate a list of folks who might be interested in the next pair of shoes or something like that. And, again, we differentiate on those use cases and apply that to all the client base that comes in and buys our products.

Senator Franken. Anything to add, Mr. Harvey or Ms. Dixon?

Mr. Harvey. I would say -- I would just point back to the minimum requirements for the data. When Mr. Caserta was talking about his risk product and how they were going off of these use cases, I would just like to point out that I would want to hope and I would probably assume that all of the data is both -- the disk is encrypted, the data when it is in the database is encrypted, and while it is being transported into the area or the holding cell that the customer comes into to grab or feed, that it always remains encrypted.

As I said earlier -- and I think Mr. Caserta has done a good job in talking to us about how seriously to consider the data, but I would want it applied to all data brokers, that all sensitive data, whatever the definition is, is always encrypted, but realize, from a legislative point of view, it is not a silver bullet.

Ms. Dixon. So just very quickly, it is incredibly important to understand that access control is one of the great Achilles's heels of all data brokers and typically what we have seen in our research is that individuals who are trying to get a lot of information about -- criminals, who are trying to get a lot of information about individuals, they will layer their efforts.

In other words, they will use one database here, one data broker there, and they will combine the information

that they are looking for.

At one point in 2005, a very famous data breach occurred. This was by ChoicePoint, where a fraud ring purchased access to background data checks and this is the exact kind of access control problem that data brokers have to deal with.

So a legitimate use, that of employment, can be spoofed very easily. So remote access, that is the big thing I think that we need to really look at in terms of immediate security issues with respect to your question.

Senator Franken. Thank you. Thank you again, Mr. Chairman.

Senator Flake. Thank you all. This has been very enlightening. As we move forward on this, we are going to need help from people like you to help us navigate this and I appreciate the candor you express.

Thank you for being here from one of the companies. Also, this is difficult stuff. What may not be sensitive as one item in the aggregate becomes sensitive and these are the things that make it difficult to legislate and to navigate.

So thank you for being here. Thank you for your testimony.

The hearing record will remain open for 1 week. Members who were not here may submit questions for the

record. We ask you to promptly respond to those, if you could. So thank you for being here.

With that, the meeting is adjourned.

[Whereupon, at 4:06 p.m., the hearing was concluded.]

C O N T E N T S