

PRIVACY RIGHTS AND DATA COLLECTION IN A DIGITAL ECONOMY

HEARING

BEFORE THE

COMMITTEE ON

BANKING, HOUSING, AND URBAN AFFAIRS

UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ON

EVALUATING CURRENT APPROACHES TO DATA PRIVACY REGULATION,
INCLUDING THE EUROPEAN UNION'S GENERAL DATA PROTECTION
REGULATION, AND ITS APPLICATION TO FINANCIAL INSTITUTIONS

MAY 7, 2019

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



Available at: <https://www.govinfo.gov/>

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama	SHERROD BROWN, Ohio
PATRICK J. TOOMEY, Pennsylvania	JACK REED, Rhode Island
TIM SCOTT, South Carolina	ROBERT MENENDEZ, New Jersey
BEN SASSE, Nebraska	JON TESTER, Montana
TOM COTTON, Arkansas	MARK R. WARNER, Virginia
MIKE ROUNDS, South Dakota	ELIZABETH WARREN, Massachusetts
DAVID PERDUE, Georgia	BRIAN SCHATZ, Hawaii
THOM TILLIS, North Carolina	CHRIS VAN HOLLEN, Maryland
JOHN KENNEDY, Louisiana	CATHERINE CORTEZ MASTO, Nevada
MARTHA MCSALLY, Arizona	DOUG JONES, Alabama
JERRY MORAN, Kansas	TINA SMITH, Minnesota
KEVIN CRAMER, North Dakota	KYRSTEN SINEMA, Arizona

GREGG RICHARD, *Staff Director*

LAURA SWANSON, *Democratic Staff Director*

JOE CARAPIET, *Chief Counsel*

BRANDON BEALL, *Professional Staff Member*

ELISHA TUKU, *Democratic Chief Counsel*

COREY FRAYER, *Democratic Professional Staff Member*

CAMERON RICKER, *Chief Clerk*

SHELVIN SIMMONS, *IT Director*

CHARLES J. MOFFAT, *Hearing Clerk*

JIM CROWELL, *Editor*

C O N T E N T S

TUESDAY, MAY 7, 2019

	Page
Opening statement of Chairman Crapo	1
Prepared statement	36
Opening statements, comments, or prepared statements of:	
Senator Brown	3
Prepared statement	37

WITNESSES

Peter H. Chase, Senior Fellow, German Marshall Fund of the United States ..	5
Prepared statement	39
Responses to written questions of:	
Senator Menendez	66
Senator Cortez Masto	69
Jay Cline, Principal and U.S. Privacy and Consumer Protection Leader, PricewaterhouseCoopers LLP (PwC)	7
Prepared statement	52
Responses to written questions of:	
Senator Menendez	73
Senator Cortez Masto	75
Maciej Ceglowski, Founder, Pinboard	8
Prepared statement	56
Responses to written questions of:	
Senator Menendez	78
Senator Cortez Masto	79

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Letter submitted by Susan K. Neely, President and CEO, The American Council of Life Insurers	82
Letter submitted by Richard Hunt, President and CEO, Consumer Bankers Association	85
Letter submitted by Jim Nussle, President & CEO, Credit Union National Association	89
Prepared statement of Rebeca Romero Rainey, President and CEO, Inde- pendent Community Bankers of America	90

PRIVACY RIGHTS AND DATA COLLECTION IN A DIGITAL ECONOMY

TUESDAY, MAY 7, 2019

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10:04 a.m. in room SD-538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. This hearing will come to order.

On February 13, Senator Brown and I invited feedback from the public on the collection, use, and protection of sensitive information by financial regulators and private companies in light of the immense growth and use of data for a multitude of purposes across the economy.

The Committee appreciates the insights and recommendations of respondents, who expressed a range of views on the topic of data collection, use, and sharing and how individuals can be given more control over their data.

Building on that effort, today the Committee will look closer at the European Union's General Data Protection Regulation, or GDPR, and other approaches to data privacy, including the impact on the financial services industry and how companies collect and use information in marketing and decisionmaking related to credit, insurance, or employment.

Providing testimony to the Committee today are three data privacy experts, including Peter Chase, Senior Fellow at the German Marshall Fund of the United States; Jay Cline, Privacy and Consumer Protection Leader, a Principal, PricewaterhouseCoopers (PwC) US; and Maciej Ceglowski—close enough?—Founder of Pinboard.

Each witness brings a unique perspective on the practical implications of implementing and complying with new data privacy laws; what has worked and what has not worked to give individuals more control over their data; and considerations for the Committee as it explores updates to Federal data privacy laws within the Banking Committee's jurisdiction.

My concerns about big data go as far back as the creation of the CFPB, which was collecting massive amounts of personal financial information without an individual's knowledge or consent.

In 2014, the GAO reported that the Bureau alone was collecting information on upwards of 25 to 75 million credit card accounts

monthly, 11 million credit reports, 700,000 auto sales, 10.7 million consumers, co-signers, and borrowers, 29 million active mortgages, and 5.5 million private student loans.

Consumers deserve to know what type of information is being collected about them, what that information is being used for, and how it is being shared.

Financial regulators are not the only ones engaged in big data collection; private companies are also collecting, processing, analyzing, and sharing considerable data on individuals.

The data ecosystem is far more expansive, granular, and informative than ever before.

As the U.S. economy becomes increasingly digital, people are using the internet, including search engines and social media, mobile applications, and new technologies to manage and carry out more parts of their everyday lives.

The digitization of the economy allows for seamless access to both more generalized and granular pieces of data on individuals and groups of individuals, including data collected, with or without consent, directly from individuals, tangentially to individuals' activities, or gathered or purchased from unrelated third parties.

In particular, data brokers play a central role in gathering vast amounts of personal information—many times without ever interacting with individuals—from a wide range of public and private sources, which is then sold or shared with others.

In 2014, the Federal Trade Commission issued a report entitled, "Data Brokers: A Call for Transparency and Accountability," in which it highlighted data brokers' big role in the economy and concerns around their transparency and accountability.

In many cases, an individual's data or groups of individuals' data is used in ways that provide value, such as risk mitigation, fraud prevention, and identity verification, or to meet the requirements of laws and regulations.

However, in many other cases, that data can be used in ways that have big implications for their financial lives, including to market or to make decisions on financial products or services that impact a consumer's access to or cost of credit and insurance products, or in ways that impact their employment prospects.

In any case, the way that an individual's or a group of individuals' data is used matters immensely.

As its rightful owner, an individual should have real control over his or her data.

A complete view of what data is collected, the sources of that data, how it is processed and for what purposes, and who it is being shared with is vital to individuals exercising their rights.

People should also be assured that their data will be reflected accurately and have the opportunity to opt out of it being shared or sold for marketing or other purposes.

In 2016, the European Union took steps aimed at giving individuals more control when it replaced a 1995 Data Protection Directive with the General Data Protection Regulation, or GDPR.

The European Union's principles-based GDPR is broader in scope, applying to a more expansive set of companies, including some based in the United States, and more types of personal information than its previous directive.

The GDPR also imposes specific responsibilities on both data controllers and data processors and enumerates rights for individuals with respect to their personal information.

In contrast to the European Union, the United States has adopted Federal laws focused on data privacy within particular sectors.

Two such Federal laws in the Banking Committee's jurisdiction are the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act.

Today I look forward to hearing more about the principles, obligations, and rights underlying GDPR and how those differ from the previous 1995 Data Protection Directive; how GDPR addresses data brokers and other companies that collect and disseminate personal information, often without an individual's knowledge, and the ways the Fair Credit Reporting Act may be adjusted to account for activities by such entities; challenges that U.S. financial institutions have faced in implementing and complying with GDPR; how financial institutions' privacy practices have evolved since its enactment; and how individuals have responded to this additional information and rights with respect to their data; whether individuals actually have more control over their data as a result of GDPR, and what the European Union did right and wrong in GDPR; and considerations for the Banking Committee as it looks to update and make improvements to Federal laws within its jurisdiction.

Again, I thank each of our witnesses for joining the Committee today to discuss GDPR, data privacy, and individual rights.

Senator Brown.

OPENING STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thank you, Mr. Chairman.

I am excited to be working in a bipartisan way with Chairman Crapo on protecting Americans' sensitive personal data—an issue everyone agrees is important.

As we start to think about this subject, we need to do it with an open mind. Technology has advanced rapidly. We should have some humility to admit that we do not even know all there is to know about what happens when personal information is collected on a large scale. As it turns out, personal information can be far more than your name, address, and Social Security number. Sometimes harmless data, once it becomes big data, can reveal big secrets, as you have all pointed out in your testimony.

Take, for example, a fitness tracking app that became popular among U.S. soldiers stationed abroad. Many of those service-women and -men tracked their daily workouts. When the aggregated fitness tracking information became public, heatmaps of common running paths revealed the locations of secure military facilities all over the world.

Even when we agree that data is sensitive, we are often not good at protecting it.

Most of us still remember the Equifax breach that exposed the detailed financial information of more than half the U.S. adult population—information that will remain useful to potential criminals for the rest of those 147 million Americans' lives.

The Equifax case reminds us that we cannot fix this by just warning people they should share less personal data on the inter-

net. People were not putting their Social Security numbers on Facebook. Equifax had collected data from various sources, and in many cases people were not even aware Equifax knew anything about them or had even heard of Equifax.

There is a lot of data floating around that can be compiled and analyzed in creative ways to make shockingly accurate predictions about our lives.

What you think of as your “personal data” is not limited to bank passwords and credit scores.

As we learned several years ago, even if you do not have a Facebook account, Facebook builds a shadow profile of your activities and your interests and your preferences from digital, shall we say, bread crumbs spread by your friends and associates online.

Sometimes you may not realize that data is being monetized. Businesses can pay to have Pokemon show up near them in the game, herding customers into their stores.

There is a common saying that “if you are not paying for the product, then you are the product.” Services that appear free make money from your personal data.

It is not easy for consumers to protect themselves. “Buyer beware” is not a particularly helpful warning since most people cannot afford to protect themselves by opting out of internet services just like they cannot opt out of banking services with arbitration clauses in them.

In today’s world, telling people to look out for themselves when it comes to protecting their personal data is about as useful as telling people to look out for themselves when it comes to food safety.

We cannot tell people to avoid the internet and avoid having their data collected any more than we can tell people to stop eating dinner. We cannot abandon the people we serve when it comes to protecting them.

If we do not take this seriously, a handful of big corporations and financial firms will continue to strong-arm customers into sharing their most intimate details.

So in addition to talking about ownership and control of our data, I hope we can talk about where Government needs to step in and create rules about the appropriate uses of personal data, regardless of whether a customer opts in. And I hope we can talk about what kind of data should be collected and should not be collected and for how long it should be stored. This problem is not just important to our personal privacy; it is also critical to our democracy. As the Cambridge Analytica scandal demonstrated, a big enough pile of seemingly meaningless data can give a bad actor ways to meddle in our elections.

The Banking Committee is responsible for one slice of the data ecosystem. I hope to work with the Chairman of Banking as well as the Chairs and Ranking Members of the other committees to set some commonsense rules on the use of Americans’ sensitive personal data.

Thank you all for weighing in.

Chairman CRAPO. Thank you, Senator Brown, and I appreciate working with you on this issue as well. It is critical to our country and to our American citizens.

We will now move to the testimony. I have already introduced each of you. I ask you to please pay attention to the clock so you can keep your oral remarks to 5 minutes. We have got a lot of Senators who are going to want to ask questions, and so we would like to have adequate time for that as well.

Let us go in the order I introduced you, and you may begin, Mr. Chase.

STATEMENT OF PETER H. CHASE, SENIOR FELLOW, GERMAN MARSHALL FUND OF THE UNITED STATES

Mr. CHASE. Thank you so much, Chairman Crapo.

Chairman Crapo, Senator Brown, Members of the Committee, good morning and thank you for providing me an opportunity to provide some perspectives on the European Union's General Data Protection Regulation—GDPR, as you have put it. My perspectives are based on over a quarter century of working in U.S.-European economic relations, including with the State Department, with the U.S. Chamber of Commerce, and now at the German Marshall Fund. My views obviously are my own.

I was asked to provide an objective description of GDPR as background, content, and implementation. My written statement, which I request be made part of the record, provides more information on each of these.

First, GDPR is in many ways unique given its context as a law of the European Union. The European Union was created to create peace in Europe after World War II, to integrate it. And the GDPR tries to bring together and find a unified basis for 28 very, very different countries on how they approach data protection, and this is to preclude them from doing things that would actually block commerce.

Second, I think it is important to remember that in the evolution of the European Union, privacy and data protection have become much more important over time, most importantly, I think, in 2009 when data protection was formally recognized and incorporated into EU law as a fundamental right.

Third, it is also important to remember that while the GDPR was being considered, the Snowden revelations came out about NSA's ability to access data held by U.S. companies, and that fueled, added to the political dynamic in the European Parliament and member states.

Although long, GDPR is simple. It lays out six principles that govern the protection of personal data in the European Union and derives from those a number of rights for individuals and obligations for those who have the data.

The principles affirm that data of any identified or identifiable person, including an IP address, must be collected and used only for specified purposes; processed in a legal, fair, and transparent fashion; limited only to what is necessary for the specific processing purposes; accurate; retained only for as long as is required; and securely protected. Of these, one of the most important is the legal basis for processing data. GDPR Article 6 provides an exhaustive list of the legal grounds on which data can be processed, with the consent of the individual, of course, which must be freely given, informed, unambiguous, and specific; to perform a contract with the

individual; to comply with the legal obligations spelled out in law; for the vital interests either of the individual or other individuals; for a public purpose, again, spelled out in law; and in the legitimate interest of the controller or a third party, as long as those interests do not supersede those of the individual. Legitimate interest is the one that is the most expansive in many ways.

Under these principles, Article 9 also prohibits the processing of any sensitive personal information, including about racial origin, sexual orientation, health, political beliefs, biometric information, unless one of 10 specific exceptions are made.

These principles lead to the rights for the individual, including the right to transparency, which get to all of the things both the Chairman and the Ranking Member mentioned in their opening statements, knowing who is collecting the data, what they are using it for, very importantly what the legal basis of any processing is, and how long it will be kept, who it is going to be shared with; access to the data that is held by companies; rectification, amendment, and even erasure; portability; and the right to object, including, very importantly, to automated decisionmaking and profiling that would be used for advertising and direct marketing.

The principles lead to obligations on the companies, including that they have to facilitate all the rights noted above. They have to have a specific legal basis for any processing. They must use technical means such as protection by design to ensure that they minimize data use. They have to conduct data protection impact assessments if they are going to process large amounts of data, particularly sensitive data or other data, in a way that would affect the rights of individuals. They have to keep records. They have to provide appropriate security. And, of course, for many companies that do a lot of data processing, they have to appoint a data protection officer.

GDPR is not a year old, but companies have spent a billion dollars preparing for it over the past 2 years, not least because the maximum fine is 20 million euros or up to 4 percent of their global turnover. So far, very few fines have been levied. The most notable one is against Google in France. This is mainly because the GDPR data protection authorities are trying to help companies comply rather than punish.

I have gone into some of the guidance documents that have been issued that have helped define some words like “contract” and “consent,” “legitimate interest,” “automated data processing.” Maybe we can talk about those in the question-and-answer period. But I thought also that it is important to note that GDPR gives organizations the right to bring—to raise inquiries into companies, and there has been a recent case, inquiry against a lot of the data brokers, including some of the financial credit rating agencies, that has been lodged in the United Kingdom in November that has not yet come out. But I think that in the end, it will take years before we have a really good sense of the impact of the GDPR. And there are some who argue that its prescriptiveness could stifle innovation to an extent. But I think that certainly companies whose business model is based on monetizing personal data, those are the ones that will probably have to take care.

Thank you. I look forward to your questions.

Chairman CRAPO. Thank you.
Mr. Cline.

**STATEMENT OF JAY CLINE, PRINCIPAL AND U.S. PRIVACY AND
CONSUMER PROTECTION LEADER, PRICEWATERHOUSE-
COOPERS LLP (PWC)**

Mr. CLINE. Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee, I appreciate the opportunity to appear today as the Committee considers privacy rights and data collection in a digital economy. As previously mentioned, my name is Jay Cline, and I am the U.S. Privacy and Consumer Protection Leader at PwC. I appear before you today on my own behalf and not on behalf of PwC or any client. The views I express are my own.

My oral testimony today will highlight some of the observations contained in my written submission to the Committee on the experience of U.S. financial institutions with the EU General Data Protection Regulation. It is an experience marked by large-scale technical and organizational change to afford new privacy rights to EU residents in an evolving regulatory environment. It is my hope that my testimony will be useful to the Committee as it considers the collection, use, and protection of personally identifiable information by financial regulators and private companies in the United States.

GDPR caused many U.S. financial institutions operating in Europe to undertake their largest-scale privacy program initiatives in two decades. Beginning after the ratification of the GDPR in April 2016, these initiatives often rivaled the scale of U.S. financial institutions earlier mobilizations to prepare for the Privacy Rule of the Gramm-Leach-Bliley Act and other related U.S. data privacy laws and regulations.

I think it is worth noting that the GDPR's requirements are focused on individual rights and program accountability and do not introduce detailed information security specifications. It is more of a data privacy law than it is a security law, as we understand those terms in the United States.

My written testimony provides more detail on lessons I learned helping financial industry clients implement privacy programs. I would like to take a few minutes to discuss some of those observations.

Almost 1 year since the GDPR implementation deadline of May 25, 2018, some top industry challenges identified for your consideration include completing a data inventory. To comply with the GDPR's record of processing requirement, U.S. financial institutions embarked on extensive projects to record details about thousands of applications, databases, devices, and vendors. These initiatives involved thousands of labor hours and in turn became the foundation for providing Europeans their new rights of data portability and erasure.

Another top challenge of the GDPR was the 72-hour data breach notification requirement. A challenge for all companies was providing meaningful notifications to regulators within a relatively short period of time within which forensics investigations would normally still be underway. Sometimes after 72 hours of detection

of a potential incident, for example, there are more unanswered questions than confirmed facts.

Two operational insights I have submitted for the Committee's consideration about the initial experience of U.S. financial institutions with the GDPR include:

First, some privacy rights appear more popular with individuals than others. The GDPR provides eight privacy rights for individuals, but when European residents started to exercise their GDPR rights after May 2018, those most chosen in my experience generally were the rights to access, erasure, and objection to use for marketing.

Second, a formalized data governance program is critical for data privacy success and forward progress. The GDPR emphasizes the need to have strong controls for personal data throughout its life cycle of collection, storage, use, disclosure, and deletion. Because personal data often moves horizontally across vertically structured financial institutions, there is a heightened need in the financial industry to identify data governance leaders and develop enterprise plans for data use that support privacy regulatory compliance.

I would like to share for the Committee's consideration one major unanswered question many of the clients I serve are struggling to answer during their long-term planning initiatives. That question is: Will the GDPR become the global standard? To plan for a future where consumers around the world may generally expect the core rights of access, correction, and deletion, many U.S. financial institutions are redesigning their privacy organizational models and capabilities as a contingency.

However the Committee chooses to address these difficult questions, I submit to you that the highest level of privacy protection in the digital age will result when both companies and consumers exercise their roles to the fullest.

Thank you for your time, and I look forward to your questions. Chairman CRAPO. Thank you very much.

Mr. Ceglowski.

STATEMENT OF MACIEJ CEGLOWSKI, FOUNDER, PINBOARD

Mr. CEGLOWSKI. Thank you, Chairman Crapo, and to the Committee for inviting me to speak today. My name is Maciej Ceglowski. I run a small online business called "Pinboard," and I operate what in Silicon Valley is considered an extremely exotic business model. I take a small amount of money, \$11 a year, for a useful service.

As you know, in my world the economic basis of the internet is mass surveillance. We all have some sense to the extent to which our behavior is being constantly monitored, not just the data we provide to the services that we use, but the observations that computers make about us in every aspect of private and public life.

This data is simply not regulated. As a tech person, I am not used to wearing a necktie. Putting mine on this morning, I saw that there was a small tag on the back of it. I realized that my necktie is better regulated than my entire industry. We collect this data. We have no transparency in what we do with it. And we are simply deceiving the American people because, as a technologist, I know that we lack the technical capacity to keep large collections

of user data safe over time. And I think you have seen in the news the litany of data breaches year after year, time after time, whether from industry, from Government. It is simply easier to attack computer systems than it is to defend them, and that reality is going to hold for the foreseeable future.

I worry that we are in the same position as the nuclear industry was in the early 1950s. We have an amazing new technology with real potential, but we are not being honest about the risks and our incapacity to store a wasteful and harmful byproduct for periods of time much longer than how long the companies storing them have existed. The last reactor in the United States was built in 1977, and the reason that we do not have new ones is in large part because we do not have the public trust.

As a small business man in a big industry, I worry that we are losing the trust of our users. It is hampering our ability to innovate because every time someone uses a computer service or product, they have to ask themselves: What am I giving away? Where is it being stored? And they are not getting clear answers. People are being asked to make irrevocable decisions about their online lives over and over again.

The pattern that I have seen in my industry is one of deceit. We are not honest about what we collect, the uses we put it for, and we are ashamed, frankly, of our business models. I am not ashamed of mine. Like I said, I take a small amount of money, I provide a service, and if you do not like it, I refund your \$11. But you will never get someone from Google or Facebook to speak honestly about what it is they are actually doing with our data and the uses they put it to. Instead, what Silicon Valley seeks to do is evade. They see a regulation, and they find a way around it. We do not like banking regulations, so we invent cryptocurrency and we are going to disrupt the entire financial system. We do not like limits on discrimination in lending, so we are going to use machine learning, which is a form of money laundering for bias, a way to blame mathematical algorithms for the desire to simply avoid rules that everybody else has to play by in this industry. And we see now that Facebook is about to enter the banking system again through the side door by releasing its own cryptocurrency.

I worry about this because Silicon Valley has been a force of dynamism. It is one of the great success stories of American capitalism, and we are putting it at risk right now by not having sensible regulation in place that creates the conditions for innovation.

I came to the United States as a kid from communist Poland, and I remember calling my father sometimes, a very expensive phone call, and every few minutes it would be interrupted by a recording that said, "*Rozmowy kontrolowane*," and that was the Polish Government informing us that the conversation was being listened to by the secret police. At least the Polish state had the courtesy to say that it was eavesdropping.

[Laughter.]

Mr. CEGLOWSKI. We should at least give people that courtesy, have openness into what is being collected, what is being done with it, and give some sense of agency so that people no longer feel like their data is being extracted from them, and we can have new busi-

ness models and a new flourishing again of innovation in an industry that was once famous for it.

Thank you very much.

CHAIRMAN CRAPO. Thank you very much, Mr. Ceglowski.

I will start out with the questioning, and there is so much to ask, I am only going to get a couple of my questions in. But I would like to start on the question of—I appreciate the description of the European Union’s system as one giving rights to individuals and obligations to those who collect and manage data.

With regard to the right, one of the rights that I think is most central is that people should be allowed to give consent to the use of their data. There is a lot of privacy consent requests going around in the United States, probably more in Europe, but I have had the experience of looking at the privacy statements that different companies or internet websites use where you give consent and agree to move forward. They are phenomenally long. They are incomprehensible. And when you do get to the actual parts of them that say what data is being collected, the description is like meaningless.

One of the questions I have—oh, and some of them say, “You cannot go forward unless you agree,” so you cannot even access the site unless you agree to something that is giving you virtually no information.

How is it handled, is this issue handled—how is the consent required to be obtained in the GDPR? And how is that working? Anybody. Mr. Chase?

Mr. CHASE. There is a requirement to make sure that individuals know what information is being collected on them. There is a specific requirement that the descriptions of the privacy obligation be done in a way that is easy to understand, clear language, and I think that what they are trying to do is trying to say you can put it up front in very useful language, but then if people want to go deeper, they can, rather than being addressed with 10-hundred pages of something that is incomprehensible. So they are talking a lot about the presentation.

It is interesting, though, that the European Union, because it requires consent for a specific and each specific use, in a way you can get many more questions, but they are supposed to be clear. It is going to be interesting to see how all of that is balanced between them.

One of the things for the requirement for specific, informed, unambiguous consent is that you are not meant to bundle things. So if you are entering into a contract with someone, you need to get permission to use or you need to tell them what information they need for you to objectively undertake that specific contractual purpose. You cannot tie that to also collecting information, by the way, to provide to data brokers. And it is interesting how that requirement for specific consent has been spelled out.

Chairman CRAPO. All right. Thank you.

I will just use the rest of my time to follow up on this and invite anyone on the panel to respond to this. But you just kind of referred to it, Mr. Chase, in your last comment. There are a lot of folks who collect data on individuals who do not actually interact with the individual. So, obviously, the individual is not being

provided a very clear, obvious consent opportunity. How is that issue addressed in the GDPR or how should we address that issue?

Mr. CEGLOWSKI. Senator, I went to visit a weather website from an EU IP address. I was asked to opt into 119 separate services and trackers.

Chairman CRAPO. I have had the same experience. Go ahead.

Mr. CEGLOWSKI. The consent requests become disempowering. I am an expert in the domain. I do not understand what I am consenting to, and I spent an hour reading all of the materials. So I think it is being used as a bludgeon against users and saying, "Hey, you wanted regulation? Well, here you have it. Everything is less convenient." And I see it as a weapon by the people who really do not want their data practices to be closely examined.

Chairman CRAPO. OK. Mr. Cline, were you interested in commenting?

Mr. CLINE. Yes, Mr. Chairman. Thank you for the excellent question. In the GDPR, you see a model that you see in many privacy laws around the world where there is a combination of an opt-in and an opt-out approach, where the opt-in threshold is set for the most sensitive or important data processing. For example, the collection of sensitive personal data requires an explicit consent or the sharing with third parties for secondary purposes requires an opt-in consent. I think Mr. Ceglowski presented testimony, in his written testimony, that even the opt-in approach has its limitations if you do not understand all of the things that you are reading.

So what I think is useful and the model I personally like and advise clients on is like when you download an app on your phone, it asks you if you allow that app to act as your contacts or track your geolocation. Even my kids understand this. I like how it is unbundled and presented in a short question. And so I think that is the challenge, is how to present these questions simply and understandably.

Chairman CRAPO. Thank you.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

Mr. Ceglowski, let me start with you. There is a concern that data collection does not just hurt individuals' privacy. You cite in your testimony a New York Times experiment, a sort of inadvertent New York Times experiment, and in light of recent reports, the entire staff of the New Orleans Times-Picayune lost their jobs. We know what has happened to print newspapers around our country.

Does the shift to targeted online advertising and data collection contribute to that decline?

Mr. CEGLOWSKI. I very much believe so. We had a business model for many, many decades where ads were targeted to content, and that was lucrative and fine. We had a show about Batman. They paid for the Batmobile with advertising that was targeted to content. They paid the salaries of the people on that production.

As the targeting has shifted to individuals, we have seen that the money has started pouring into the ad networks first and ultimately Facebook and Google. It is a great shift of revenue away from publishers, and the New York Times experience shows what

we suspected, that this is—publishers are better off without the targeted advertising.

Senator BROWN. It has not changed behavior?

Mr. CEGLOWSKI. Behavior by whom?

Senator BROWN. Behavior by the newspaper industry?

Mr. CEGLOWSKI. Very much so because the newspapers are now targeting—every article has metrics on it, so every time you publish something, you have to chase clicks, you have to chase eyeballs. It creates different incentives for reporters, for editors, and it takes away their power, the very basic power of the purse. Their revenue comes from an outside source, and they have to do whatever—

Senator BROWN. They change their behavior online, not change their behavior in print.

Mr. CEGLOWSKI. The print edition now follows the online edition, so the newsroom behavior is affected very much by the economics of it.

Senator BROWN. You said machine learning is money laundering for bias. Would you explain that?

Mr. CEGLOWSKI. That is correct, because machine learning algorithms are opaque. You feed them data, but then their behavior is not something that you can open the hood and look at the workings of and explain. It becomes a powerful way to circumvent restrictions. So, for example, if I wanted to lend only to women in their 30s who do not have a child and are not going to have a child, there are laws in place that prevent me from doing this directly, but if I can train a machine algorithm on enough data that it can identify those people without looking at any of the protected categories, I have effectively evaded the regulation, and my hands are clean if I do it in a clever enough way. So that is the sense in which I mean it.

Senator BROWN. GDPR focused on giving individuals ownership and control of their personal data. Is that working?

Mr. CEGLOWSKI. I think it is too soon to tell, and I would defer to the people who know more.

Senator BROWN. Anybody else? Too early? Mr. Cline? Mr. Chase?

Mr. CHASE. One of the things GDPR was supposed to do was to increase trust in the internet and, interestingly enough, trust in the internet has actually been going down since the implementation of GDPR, probably because people are becoming more aware of what companies do.

So the question will be whether or not they start acting on that, and I think that there is some indication that they are.

Mr. CEGLOWSKI. I would say it is hard to trust foreign companies from the perspective of a European. Imagine if every online service was provided by people from outside the United States how we would feel trying to regulate it and seeing it not regulated at home.

Senator BROWN. Mr. Ceglowski, one more question. Is there any entity, public or private, that has done a good job protecting people's sensitive data over a long period of time?

Mr. CEGLOWSKI. I think the closest we have seen to that is the IRS. However, even they, I believe, were infiltrated by Scientology at some point in the 1970s. I do not recall the details. But that is the best example I can think of. Basically highly regulated indus-

tries and Government have done the best job that they could, but even they have slipped.

Senator BROWN. A handful of huge tech companies have dominated the data collection landscape. Can regulation give small businesses the ability to compete with them?

Mr. CEGLOWSKI. Absolutely. Small companies in the sector, they cannot compete on price when things are free. They cannot compete on engineering when, you know, they are outnumbered. But they can compete on privacy very effectively. We need the tools, however, to be able to compete on privacy, and those tools include some legal basis for making credible commitments to customers. Right now we just have terms of service that can change at any time. But if there was a basis in law where I could commit to certain privacy practices and my users could believe that commitment because I would go to jail if I broke it, I think we would see a flourishing of innovation and privacy-friendly smaller companies.

Senator BROWN. Thank you.

Chairman CRAPO. Thank you.

Senator TESTER.

Senator TESTER. Thank you, Mr. Chairman and Ranking Member Brown, for having this hearing. Thank you all for being here very, very much.

I think that some of you have pointed out, if not all of you, that the public trust is being lost, and I could not agree with you more, and it is somewhat distressing.

I want to touch a little bit on the consent forms. I have the impression—and correct me if I am wrong—that the consent forms are complicated because there is an agenda behind them. They could be made much more simpler if they wanted to. Is that correct? I am talking about the consent form to opt in or opt out on whether you want your information shared or utilized.

Mr. CEGLOWSKI. I believe part of the complexity is the extreme complexity of the middlemen intermediaries, data brokers, ad networks.

Senator TESTER. So let me ask you this: Why can't there just be a consent form at the beginning, similar to what I think Mr. Cline talked about, that just says, "Will you allow me to use your information in any way that I want? Yes or no."

Mr. CEGLOWSKI. That is the de facto state of affairs.

Senator TESTER. And so why isn't it that way? Why can't we regulate it to that effect? What is the downside of saying, "You know what? Your consent form statement is going to be clear," just like a pack of cigarettes, "This will kill you," basically is what it says on it. Why can't we do the same thing with the internet, with the websites that we use, with the programs we use?

Mr. CEGLOWSKI. Because one aspect of consent is the ability to say no, and we really do not have that ability. Opting out of the online world is really not an option for anybody.

Senator TESTER. So what you are saying is even if they—in the consent form, if you had—if we required that at the very beginning, if you are working on—if you are utilizing Wells Fargo's bank account, it says, "You cannot utilize this information except for me, my purposes," in other words, if I want to get on a website, I can, but you cannot export it to anybody else, that is impossible?

Mr. CEGLOWSKI. That is a very different question. They are only allowed to use the data for themselves.

Senator TESTER. Yes.

Mr. CEGLOWSKI. It is very different from the current——

Senator TESTER. Right. It would change the current system.

Mr. CEGLOWSKI. Understood.

Senator TESTER. Could it be done?

Mr. CEGLOWSKI. It would have an enormous impact on the online economy, but it could be done.

Senator TESTER. And so you think it would tank the online economy?

Mr. CEGLOWSKI. As currently built around collecting all information about everybody, yes.

Senator TESTER. OK, but would—I know, but does that mean it would tank the economy?

Mr. CEGLOWSKI. We would bounce back.

Senator TESTER. OK. That is better.

Mr. Chase?

Mr. CHASE. You know, there is a lot of discussion about consent. In the GDPR, there is a difference between transparency, which the consumer should always know what is happening——

Senator TESTER. Right on.

Mr. CHASE.——and consent as a legal basis for processing data. So there are a number of different legal bases, and it is interesting because the data protection supervisors have basically said consent in some ways is the least useful way of doing it because it means that there is no other legal grounds for processing the data. And it was an interesting way that they put it.

But getting back to Senator Crapo's earlier comment, when a company scrapes all my information off the internet and then creates something with it, they actually have to inform me that there is a whole article about indirect collection and processing of data. They have to inform me that they are doing it either when they have collected it or when they, for instance, sell that information, sell my clients——

Senator TESTER. This is through the GDPR, you are talking about?

Mr. CHASE. Yes, that is correct.

Senator TESTER. And how do they inform you?

Mr. CHASE. They have to write to you and make a public announcement——

Senator TESTER. And what happens if you do not like it?

Mr. CHASE. Particularly if it is being used—you can object. You can object to the data processing——

Senator TESTER. And did they stop it then? Does that stop it from being shared?

Mr. CHASE. If they do not stop, then they have to——then they are liable to fines.

Senator TESTER. All right. So this is for anybody who wants to answer it. There were a couple breaches that were pretty high profile, in Target and Equifax. Would the outcome of—I do not know if you are familiar with them or not, and if you are not, that is fine. But would the outcome of those situations have been different here

if GDPR had been—if something like GDPR had been implemented?

Mr. CHASE. Just very briefly, Europe has lots and lots of data breaches as well. The existence of GDPR does not stop it. But if companies—

Senator TESTER. Has it reduced it? Or has it not been in effect long enough to know?

Mr. CHASE. Actually, reports of data breaches have been going up because people are over-interpreting the requirements of the law.

Senator TESTER. Well, I have got a whole bunch of stuff on this. I have just got to tell you that I am really, really, really old school. In fact, when I get out of this job, this baby [indicates phone] is going away, OK?

[Laughter.]

Senator TESTER. Because I do not like people tracking me on it, and I say “Do not track me,” but I am not sure that has any effect. I do not like when I use a website that I get telephone calls from telemarketers on something entirely different, which is total B.S. And I just think we have got to—the point that was made that we are losing the public trust is critically important. I think the internet can be used to do some marvelous things and is being used to do some marvelous things. But I think there are other people out there—and their names have already been mentioned—that are using it to make themselves into billionaires, and I get no benefit from it. All I get is the nuisance of all this B.S.

Thank you.

Chairman CRAPO. Thank you, Senator Tester.

Senator Warner.

Senator WARNER. Thank you, Mr. Chairman and Ranking Member Brown.

Before Senator Tester leaves, I think, you know, you have hit on the right things. But the first-party consent alone is not going to get it done. I would argue that particularly some of the social media platform companies use levers of psychological manipulation that would blow you away no matter how clear-cut your first consent form is. So I have got legislation with Deb Fischer called “The DETOUR Act,” which basically looks at the dark patterns and the tools these platforms use to psychologically manipulate. The 17 arrows pointing at “Click here, I agree,” and you can never find “Unsubscribe” is the most kind of basic notion. And we do need some rules of the road in this space and some guardrails, I would argue. This would be *de minimis*, a starting point.

Your questions to Mr. Chase, GDPR would not stop the negligent behavior of Equifax. The fact that we are almost 2 years after Equifax, 150 million Americans’ personal information out there. They took a small dip in the stock price, and that there has not been a penalty paid in terms of a fine is outrageous. The fact the stock has recovered and this is being built into the cost of doing business—and the FTC is going to come out a little bit later, sometime over the next couple of weeks, and do a few billion dollar fine on Facebook. Facebook makes \$18 billion a quarter top-line revenue. If we do not find a way to put some rules of the road in place—you think you are getting hosed now?

Senator TESTER. I know I am getting hosed now.

[Laughter.]

Senator TESTER. The problem is there has got to be some way to stop it. And, by the way, psychological warfare is one thing, but it is tough to do that when there is not a lot of psychology—

Senator WARNER. Well, let us go with Mister—your last name, sir, again?

Mr. CEGLOWSKI. Ceglowski, sir.

Senator WARNER. And for the whole panel, but one of the things that makes me crazy is that a number of individuals think, “Oh, gosh, Facebook, Twitter, Google, they are free.” They are not free at all. They are giant sucking sounds, sucking personalized data out from each and every one of us, and then marketing that to a whole series of entities. I know there are people that are grossly concerned about what the Government knows, but if the KGB had had the kind of data collection tools that Facebook and Google and Twitter have, the Soviet Union would have never fallen because they would have been able to have that level of control. And they will shortly have this level of control in China because the Chinese Communist Party does scrape the information from Alibaba, Baidu, Tencent, and a host of other companies most of us have not heard of.

So starting with you, sir, is there not a way, if we put requirements in place, that we could have—I am going to give you three notions.

One, shouldn’t our data be portable? As a former old telcom guy, it used to be really hard to move from one telco to another until we did number portability. Shouldn’t we have data portability? We are tired of Facebook? Shouldn’t we be able to pick up and move all our data in an easily usable form to another platform?

Two, shouldn’t we have a right as a consumer to actually just know what data points are being collected on us on a regular basis and easily access that?

And, three, because I want to make sure I get everybody on the panel to respond, shouldn’t we know—and this is kind of the Holy Grail, but I think they will end up giving you the data points. But the Holy Grail is we should know what that data, our personal data, how much that is worth on a monthly or quarterly basis to a Facebook, a Google, or a Twitter. And they will say they cannot give you that. Baloney. We have got documents that show that. But shouldn’t we be able to know portability, what the data points are, and data valuation?

Mr. CEGLOWSKI. Being able to download data, absolutely, we should have that right.

Portability is a tricky issue in a situation where you have an oligopoly because what you will have is you will have companies like Facebook that dominate a market, they will just suck the rest of the data in, and they will find ways to undercut anybody—

Senator WARNER. Well, portability along with interoperability, because you do not want to be able then not communicate with people who are on the previous platform.

Mr. CEGLOWSKI. I think in principle it is a great idea, but it can lead to further concentration.

And then finding out where the money is coming from, these free services that have lavish headquarters, I would love to know what the real Facebook business model is——

Senator WARNER. Or how much your data or my data—yours may be worth 15 bucks a quarter, and mine may be worth 12.

Mr. CEGLOWSKI. At what point does it go “ka-ching,” I would love to know that.

Senator WARNER. Well, part of it would be that would also potentially allow people to disintermediate because there might be a business proposition.

Mr. Chairman, could I get the other two to answer? And I will not say another word.

Chairman CRAPO. Yes, please do answer. I want to know your answers. But we need to keep moving.

Mr. CLINE. Senator Warner, thank you for your question. I think it gets to the heart of the answer, the heart of the issue. From my experience helping primarily banks and insurance companies get ready not only for GDPR but laws around the world, I have seen some commonalities go in the direction that you indicated. So, for example, the GDPR, the California Consumer Privacy Act, the Fair Credit Reporting Act, and other privacy laws around the world do share one thing in common: giving people a right to access their data. GDPR and CCPA also share a right to delete data. And the financial institutions that I serve that are operating globally are making contingency plans for the day when people worldwide will expect these rights, whether or not they are legally required in the jurisdictions where they live. So there is a customer experience question that the clients I serve are dealing with.

Mr. CHASE. I have nothing further to add. It has been pretty much covered.

Chairman CRAPO. All right. Thank you.

Senator Warren.

Senator WARREN. Thank you, Mr. Chairman.

So companies like Equifax vacuum up and profit from mountains of sensitive data, including Social Security numbers, passport numbers, driver’s license numbers, and there is no way for consumers to say, “No, thanks. Leave me out of this.” You need a credit report to buy a home, to rent an apartment, even to get a job nowadays.

So consumers also cannot withhold the information. Banks and other companies send it directly to credit report agencies, which package it together and then sell it for a profit.

So 20 months ago today, Equifax announced that hackers broke into the Equifax treasure trove and ransacked it. The hackers stole personal and sensitive information for almost 150 million people. So, Mr. Ceglowski, millions of American families are struggling to figure out how to protect their identities in the wake of this hack. My office issued a new report showing that Equifax-related complaints to the CFPB have nearly doubled since the breach was announced, but data like birth dates and Social Security numbers cannot be changed easily in order to thwart the scammers or identity thieves. Is there any way to actually put consumers back in the position they were in before the hack?

Mr. CEGLOWSKI. No. That ship has sailed, and it holds even more for the OEM hack where you have very sensitive questionnaires

that were leaked about people with security clearances. That is going to have an impact for decades.

Senator WARREN. OK. So once the data has been stolen, families are vulnerable to identity theft basically forever. My office launched an investigation a week after the breach was announced and found that Equifax routinely failed to patch known cybersecurity vulnerabilities, including the one that was exploited by the hackers in this breach 20 months ago. The company also failed to segment data into different systems, meaning that once Equifax's outward defenses were breached, hackers had access to almost everything.

Mr. Cline, you advise a lot of companies on cybersecurity. Are these the types of practices that you would expect to see at a company like Equifax that holds huge troves of sensitive data?

Mr. CLINE. Senator Warren, I appreciate your question. My experience is in helping financial institutions build the privacy controls and privacy rights for laws like GDPR and not so much on cybersecurity. But it is my experience that writing a foolproof privacy policy is difficult because hackers keep changing their tactics. The company—

Senator WARREN. I am sorry. The question was just pretty simple. You know, they did not patch known vulnerabilities, and once you got in, you could go through the whole thing. Is that what you would expect from a company like Equifax or any security company that has this kind of sensitive information? Is that what you think is best practices?

Mr. CLINE. I think the companies I have seen have the most success preventing breaches are those—

Senator WARREN. That is not the question I am asking. The companies that have the most success preventing breaches are those who do a better job. The question I am asking is: Did Equifax follow best practices here?

Mr. CLINE. I—

Senator WARREN. I will take that as a no. You are saying that it was—so let us think of it this way. It does not surprise me that Equifax is not doing this. For companies like Equifax, hardworking Americans are products. They are revenue sources, bundles of information to sell. And it does not matter if the customers get hurt. As long as the consumer data are still there and they can sell it, Equifax will keep doing fine. And unless companies actually take a financial hit when there is a breach, there is no incentive for them to invest in cybersecurity.

So we are now a year and a half out from the Equifax breach, and what has happened financially to Equifax? According to Bloomberg, the company suffered “no major defections” of clients and with a year of the breach was on track to make record profits. Equifax's revenue went up by over \$200 million in 2017 and went up by another \$50 million in 2018. And the Federal agencies that have jurisdiction over the breach, the FTC and the CFPB, have done nothing. Equifax put nearly half of American adults at risk of identity theft for potentially the rest of their lives, and they got away with it.

I have a plan to change that. Senator Warner and I are reintroducing the Data Breach Prevention and Compensation Act, which

will impose mandatory penalties on credit reporting agencies for every piece of data they lose and will compensate the victims. The bill will also give the FTC new tools to help keep data safe.

The only way the credit reporting agencies are going to adequately invest in cybersecurity is if we make it too expensive for them to ignore, and Congress should pass our bill.

Chairman CRAPO. Senator Smith.

Senator SMITH. Thank you very much, Chair Crapo and Ranking Member Brown. And I want to thank all of you for being here, especially thank my colleague from Minnesota, Mr. Cline, for joining us today. I appreciate that.

So, you know, as I listen to this, it just seems so clear that this system, this business model, is set up for the benefit of the data and tech companies, and basically our personal data is basically fuel for this incredible money machine that has been created. And the GDPR is attempting in Europe to set up some guardrails to protect how that data gets used and what people know about their data, but yet it seems that that is sort of layered on top of this system that is for the benefit of making tons of money off of people's personal data.

And so my question is: First of all, if the GDPR were to become the global standard, do you think that that would solve our challenges here? And I know you think it is a little too early to say, but do you think that that is going to fix this issue for us?

Mr. CEGLOWSKI. I would say that the GDPR is an important step, but it is not adequate basically because of this problem of consent. How do you consent to something that you do not even understand?

Senator SMITH. Right.

Mr. CEGLOWSKI. How can you withhold consent in a world where you have to be online? So I think that is the challenge that the GDPR does not address?

Senator SMITH. As somebody said, you know, it has created more friction, I think, for the user, but fundamentally it is just—I think you said it is like this baroque system of consent that is completely confusing to everybody. Mr. Chase?

Mr. CHASE. GDPR recognizes that direct marketing is legitimate, but it does create, I would say, frictions in a lot of how that is done, and it does create a very strong ability for customers to opt out of it—not to opt out of advertising *per se*, because it is advertising that brings in the revenue, but to opt out of personalized advertising. And so I think that that distinction is interesting.

Senator SMITH. So what if we were to set up a system that actually put privacy—you know, either a system that allowed for companies to compete on privacy or required them to compete on privacy, what would that system look like?

Mr. CEGLOWSKI. One very effective place to begin is to put limits on the amount of time that you can retain data. So if you are hoovering up everything in the world about people, at least do not store it permanently, reduce the chances of a breach, and it means I can try your service without forever for my lifetime knowing that you know my location or that you keep recordings of what I said into the home microphone that you sold me.

Senator SMITH. So a lot of that is around how long you save the data, and that would be a system that rewards protecting privacy. What would be some other things that we could do? Anybody.

Mr. CLINE. Senator Smith, it is an honor to meet you in our Nation's capital. I can point to two things that I have seen in operation that have moved things in a positive direction as a result of the GDPR. The GDPR elevated two industry best practices to the status of regulatory requirements: completing a data inventory and conducting privacy impact assessments.

Now, these things are not seen by consumers, but they are happening in the background, and they are necessary in order to provide privacy rights. I encourage my clients to do these two things whether or not they are legally required because they are so essential for giving transparency and having control over the data they have.

Senator SMITH. OK. Thank you.

I want to just switch to another topic which I think is really interesting. Mr. Ceglowski, you talk about how tech startups in the highly regulated areas of health, finance, and banking, how they should be required to compete on the same regulatory footing as established businesses in those areas, and so think about the data privacy laws that are required around HIPAA, for example, yet you note in your testimony how machine learning can identify based on people's images on Instagram whether or not they are likely to be suffering from depression, and what they do with that learning is not guided by HIPAA. The same issues in another category of financial services about how machines can decide whether or not you are eligible for a loan, but you do not have the same credit protections.

What should we do about that? Where does that lead you in terms of what steps we ought to take?

Mr. CEGLOWSKI. I think the issue here is that those protections were determined by democratically elected representatives. They represent years of effort and thought, and they are being circumvented by people who are accountable to no one. So introducing the accountability so that regulation about how machine learning is used does not come from idiosyncratic founders but it actually part of the regulatory conversation is important. But that principle that you do not get to go around regulation you do not like I think is a vital one.

Senator SMITH. It is essentially a fundamental question of fairness.

Mr. CEGLOWSKI. Yes.

Senator SMITH. Thank you.

Thank you, Mr. Chair.

Chairman CRAPO. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you, and thank you, Mr. Chairman and Ranking Member, for this conversation. I really appreciate it.

Let me just follow up on some of the conversation of my colleagues. The Gramm-Leach-Bliley Act and the Fair Credit Reporting Act are two data privacy-focused Federal laws under our jurisdiction right here that we are talking about. My understanding is the privacy provisions of the Gramm-Leach-Bliley Act are really

based on two things—notice and choice model—which we have said are ineffective. Would you all agree at this point in time that there needs to be more done than just a notice and choice model? Just for the panel members, yes or no. Let us start here, Mr. Chase.

Mr. CHASE. Looking from the GDPR point of view, they would say that it is nowhere near effective enough.

Senator CORTEZ MASTO. Thank you.

Mr. Cline?

Mr. CHASE. My job is to help companies operationalize whatever Congress and the States deem is the best for the American people.

Senator CORTEZ MASTO. OK.

Mr. CEGLOWSKI. I would say yes.

Senator CORTEZ MASTO. Yes, it is effective enough, or no, it is not?

Mr. CEGLOWSKI. Yes, it needs to change. It is not effective.

Senator CORTEZ MASTO. It needs to change, right. And so you would all agree—let me ask you this: Would you all agree that the rules for the financial sector should be the same as every other broader business in the economy as well? As we address this issue with respect to data privacy and security, they should all be treated equally, including the financial sector? Mr. Chase, yes or not.

Mr. CHASE. No. If you want my personal opinion, just for—

Senator CORTEZ MASTO. Why should the financial sector be treated differently?

Mr. CHASE. The GDPR, which is what—I am trying to come in from the point of view of what the European law requires, and the European law provides an omnibus law for everything, so it provides in a way a minimum. But there can be additional requirements for some information. And there is a difference, I think, here between types of information and—focusing on types of information or focusing on institutions. I think the GDPR focuses on the type of information more than just the institution and its location.

Senator CORTEZ MASTO. OK. Mr. Cline?

Mr. CLINE. Senator, I do not have an opinion on that question.

Senator CORTEZ MASTO. OK.

Mr. CEGLOWSKI. I do not understand financial regulation enough to give a qualified answer.

Senator CORTEZ MASTO. All right. Thank you. So let me ask you this: Would you all agree that what we are trying to achieve here, it requires a comprehensive approach, is what I am hearing to addressing data privacy and security? Would you all agree with that? Is that a yes?

Mr. CEGLOWSKI. Yes.

Mr. CLINE. Yes.

Senator CORTEZ MASTO. Yes? OK. So let me ask you a couple of things. Would you support the need for, if we were looking at doing some sort of data privacy legislation, that it require entities to practice reasonable data minimization practices? Would you support that? Yes or no.

Mr. CEGLOWSKI. Yes.

Senator CORTEZ MASTO. Mr. Cline?

Mr. CLINE. I can tell from my observations in serving companies that have been helping to do GDPR, data minimization is a foundational principle for their programs.

Senator CORTEZ MASTO. That is yes. Thank you.

Mr. Chase?

Mr. CHASE. Yes, and what he said about minimization requirements under GDPR.

Senator CORTEZ MASTO. OK. And would you also agree that anything that we come up with must be for a legitimate business or operational purpose and must not subject an individual to unreasonable privacy risk? Yes or no.

Mr. CEGLOWSKI. "Legitimate" is the loaded word there.

Senator CORTEZ MASTO. OK. Mr. Cline?

Mr. CLINE. Again, I think from the European perspective, where legitimate interest is a foundational principle now under GDPR, the clients that I serve are operationalizing that principle.

Senator CORTEZ MASTO. Mr. Chase?

Mr. CHASE. That is the approach the Europeans took, and sometimes I wonder if they were actually—if they did not need a better problem definition.

Senator CORTEZ MASTO. OK.

Mr. CHASE. What was the problem they were trying to solve?

Senator CORTEZ MASTO. That is helpful. Thank you.

What about this? Would you agree that the data practices may not discriminate against protected characteristics, including political and religious beliefs? Yes or no.

Mr. CEGLOWSKI. That is a foundational American value.

Senator CORTEZ MASTO. That is a yes.

Mr. CEGLOWSKI. That is a strong yes.

Senator CORTEZ MASTO. Thank you.

Mr. Cline?

Mr. CLINE. Yes.

Senator CORTEZ MASTO. Mr. Chase?

Mr. CHASE. Of course. That is current law.

Senator CORTEZ MASTO. Thank you.

Now—and I have only got a few minutes left—let us talk about the consent piece because I think that is our biggest challenge. And I hear what you are saying today in the conversation today.

What about this? What if we were to look at kind of a bifurcated approach here and we had two things: one, we allowed entities—required entities to provide users with reasonable access to a method to opt out for data collection, processing, storage, or disclosure; but we also required affirmative opt-in consent in two circumstances: one, collecting or disclosing sensitive data, such as generic, biometric, or precise location data; and disclosing data outside the context of the consumer relationship, as I talked about earlier. Are we getting closer to addressing the consent concerns that you addressed earlier?

Mr. CEGLOWSKI. I think given the realities of machine learning, you can no longer talk about some data being sensitive and other data not being it, because you can reconstruct the sensitive data from the other stuff. So opt in across the board is what I would urge for.

Senator CORTEZ MASTO. Opt in across the board for everything.

Mr. CEGLOWSKI. For everything.

Senator CORTEZ MASTO. OK. Anybody disagree with that?

Mr. CHASE. Yes, I disagree.

Senator CORTEZ MASTO. OK. Why do you disagree?

Mr. CHASE. Because I think that there are a lot of processes that are undertaken that are not intrusive and that do not affect a person but can be useful for a company or the data processor or controller. And, also, I think that there is a question of the difference between inferred data and actual data. And to all our credits, to the technologists, not 100 percent of their inferences are right, and that is one of the problems, in fact, that they are sometimes not as good as they like to make it out to be.

Senator CORTEZ MASTO. Thank you. I notice my time is up. Thank you so much. I appreciate it.

Chairman CRAPO. Senator Kennedy.

Senator KENNEDY. Thank you, Mr. Chairman.

Do any of you disagree with the proposition that if I go on the internet and generate data that I own my data? Does anybody disagree with that?

Mr. CEGLOWSKI. I do disagree.

Senator KENNEDY. You do. OK. Well, I think I own it. I think I have a property right in it. I have a right to license it. Let us take Facebook, for example. When I go on Facebook, and in return for giving up all my data rights, I get to see what my high school friends had for dinner Saturday night. I think I still own my data. That is my opinion, anyway. But I license it to Facebook.

Problem number one, it seems to me, is the user agreement—not to pick on Facebook. Their user agreement has been improved, but for the longest time you could hide a dead body in there and nobody would find it.

Why don't we just require social media companies to write user agreements in plain English? Would that help with the problem?

Mr. CEGLOWSKI. I think that that user agreement would just say, "We are taking all your data. Yes or no."

Senator KENNEDY. Well, I think we can do better than that. Maybe you cannot, but I think most people can.

Would a clearer user agreement help, gentlemen?

Mr. CHASE. The European approach would say yes, there has got to be a clear agreement, but more than that, there are limitations on the data that can be collected and—

Senator KENNEDY. I understand that, but I want to take this—

Mr. CHASE.—and how it can be used.

Senator KENNEDY. I want to take this—well, let me just put it this way: What if we just passed a law that says, number one, I own my data, I have a property right to it. Number two, I have the right to license it, but it has to be knowing and willful. Number three, the user agreement through which I license it has to be written in plain English so that a person of average intelligence can understand it. Number four, I have the right to change my mind about licensing it. Number five, I have the right—and the social media companies can do this by just putting a simple icon on their platform. I have the right not only to know what data the social media company has about me, but the analysis, their analysis of that data. Number six, or wherever we are, I also have the right to know what the social media company is doing with my data. Number seven, I have the right to transfer my data. And, number

eight, I have the right to be notified immediately if my data is breached.

Now, what if we just did that? Isn't the problem solved?

Mr. CEGLOWSKI. It comes back to the ownership of data. If I am part of a group conversation, who owns that conversation? Is it just me? Is it evenly split between participants? That is the part that I stick on.

Senator KENNEDY. I understand. We just disagree on that. Mr. Cline?

Mr. CLINE. So I help companies write some of those privacy notices that are long and difficult, and I can say that the goal is to be extremely precise and detailed for the purpose of being very transparent and I can understand—

Senator KENNEDY. No, it is not. The purpose is not to be transparent. The purpose is to cover the rear end for the social media company. You and I both know that. Let us not kid each other.

Mr. CLINE. I approach that part of my job with that goal of transparency.

Senator KENNEDY. Well, you are paid by whom?

Mr. CLINE. My firm.

Senator KENNEDY. Who is your firm—who is your firm's client? You are paid by your client, aren't you? Isn't your client the social media company?

Mr. CLINE. I focus in the financial services industry.

Senator KENNEDY. Are you telling me that when the user agreements are written, the main purpose of the user agreement is not to protect the social media company? Is that what you are saying?

Mr. CLINE. Senator, as a private—

Senator KENNEDY. Is that what you are saying?

Mr. CLINE. That is not what I am saying.

Senator KENNEDY. OK, good. Because if you believe that, you will never own your own home because it is just not true. Go ahead.

Mr. CLINE. In the privacy profession, I think it is widely—the privacy notices are widely seen as a contract between the company and the individual.

Senator KENNEDY. I agree with that. Would my idea work, Mister—I am sorry. I cannot see that far. Peter?

Mr. CHASE. Chase.

Senator KENNEDY. Mr. Chase.

Mr. CHASE. Thank you very much, Senator. You put too many things in there at one time. The question of ownership I think is a different issue than access. The Europeans are trying to make a clear distinction between ownership and access, because I think that not all property rights come from all knowledge about me. Indeed, a lot of the public—a lot of information about me is in the public domain. It is public. It is not owned by anyone.

But more to the point, your point that companies must clearly tell customers, people, what they do with the information, who they share it with, all of that is something that the Europeans push for. Further, I think one of the things they also try to emphasize is the need to minimize the data collected and that the data is collected only for the purpose that is necessary. They would argue—they do argue, in fact, in papers—that it is not in your legitimate interest to vacuum up all the information that you can find about me.

Senator KENNEDY. Well, I will end on this note. I was in Brussels not long ago with our Chairman, and we had a meeting with a lot of the folks who are implementing the European Union's General Data Protection Regulation. They do not know what is in it. They do not know what is in it, and the people who have to comply with it do not understand it. It is a mess. I just think we need to aim for something simpler.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Reed.

Senator REED. Well, thank you, Mr. Chairman, and I must associate myself with many of the comments by Senator Kennedy. I thought he was very thoughtful and got right to the heart of the matter, so thank you.

Let me commend you all for your testimony. I was particularly impressed with Mr. Ceglowski's testimony, its eloquence and its thoughtfulness. One of the rules of thumb that I learned in the Army was, "Keep it simple, stupid." And there might be three ways in which we can deal with this issue, reflecting some of the comments before: first, require opt-in so people get the choice from the beginning whether they are going to give their data, because like Senator Kennedy, I believe people own their data, particularly sensitive data; second, as has been suggested, forget the data over a certain period of time, 6 months, a year, whatever is reasonable—probably closer to 6 months than a year—and then give people the right, if their rights are violated, to go to court and demand their rights.

Now, that is a pretty straightforward solution which I hope will address this. I think our tendency is to get into nuanced regulatory directives that are taken by agencies and further nuance so it is a fine powder and not a strong protection against privacy violations.

So first let me go to Mr. Ceglowski. Your comments?

Mr. CEGLOWSKI. I definitely agree that much of the language around regulation is intentionally obfuscatory. People do not want to show how the sausage is made, to what extent data is being used. I do think there is a degree past which we cannot simplify these things. For example, it is fine to say I own my data, but if you can reconstruct everything you want to know about me by looking at my friends, by looking at their behavior, then to what extent is that now your data or is it still mine because it is identical? Those are the kind of things that I think make it difficult to regulate here. But I welcome any attempt at simplification.

Senator REED. It seems to me that you are exactly right, but if, for example, your data expires, it disappears in 6 months, and your friends' data disappears 2 months after that, it is hard to—and, in fact, we have to take—I think what you are suggesting, we have to take a further step. The synthetic data created, the second-stage data created by this merger of data, that, too, has to be, you know, eliminated. Because I think you are exactly right. What the companies will do, create their models of the person's behavior and projections and then claim it is not the person's data, it is this synthetic data we have created. So that is in addition to what we should do.

Mr. Cline, your thoughts?

Mr. CLINE. Senator, I think the model that you have proposed is the trend that we are seeing worldwide, even outside the United States and Europe in countries like Brazil. And the clients that I serve are preparing for these trends, this very simple model.

Senator REED. Interesting, because your comments before, Mr. Cline, is that they are preparing for these trends, anticipating them, and also are expecting to still profit from their business. Is that correct?

Mr. CLINE. The clients I serve are primarily for-profit companies.

Senator REED. Many times we get this, "You cannot do this because it will ruin the internet. We will have to charge exorbitant fees. No one will get access to it." You know, there is a lot of weeping and gnashing of teeth about how terrible it is going to be, this is a free platform, *et cetera*, when, in fact, these commonsense approaches can be adapted to a profit-making enterprise that will still be significantly profitable. Is that your view? Thank you.

Mr. Chase?

Mr. CHASE. It is understandable—and it was certainly the case in Europe—that when people were regulating, they were focusing just on the large social media companies. But the internet and the people who are in this ecosystem who were involved are, of course, everyone. I have done a lot of work in the energy area. The energy system is becoming highly digitalized. When you are regulating, in order to keep it simple, you also have to realize that there are many different issues and applications of data.

Second, in terms of retention, going directly to that, if I am a member of Facebook, I want them to remember everything that I have had on there forever. I want that record. They are my custodian of my life. So—

Senator REED. You want that record until they bring up your conviction for drunken driving when you were 17-years old. That is when you say, "I did not want that"—

Mr. CHASE. Obviously, you feel that you should have the right to change the record that you have created. But I think that the point here is that—is it that they have the information or is it how they use the information and specifically if they use it toward targeting advertising or targeting messaging? And I think that this goes to the point I made earlier about not always having a clear problem definition in Brussels when they were doing the GDPR.

Senator REED. I think it also goes to—and let us be honest—the capacity of Government. If we try to go and anticipate all the myriad ways in which these companies can use information and regulate it, we will be in a disaster. I think we have to have simple rules—they work pretty good—that can be enforced effectively.

One other caveat I will make, because this is a very complex issue, is that I can anticipate some areas, for example, if you are following a group of children who have a pediatric disease, you probably want that data to stretch over many, many, many, many years because that is where you will find out what the effects are. And in that case, you can carve out an exception, which they would have to agree to, which presumably they would because they are in the trial. But it is a lot different than the purchases you are making, the locations you are driving to, things like that which are

being woven together in very intricate ways. You know, the way—again, we cannot anticipate some of the ways that this is being done, but locations are being coordinated so they can put the right sign up to advertise Adidas on the highway because they know there are, you know, crowds and crowds of 30-year-olds going to their high-tech companies that way every day. You are not going to put, you know, old people's medicines on that billboard. It is Adidas.

So I think we have got to take a very simple but very effective—we have got to do it soon. We are running out of time. So thank you.

Chairman CRAPO. Thank you.

Senator Jones.

Senator JONES. Thank you, Mr. Chairman. And thank you to the witnesses for coming here.

Just to follow that up a little bit, Mr. Ceglowski, this whole thing about inferences, a world of inferences, and everything that Senator Reed was talking about, are we actually having the wrong conversation? If all companies, if all they need is publicly available data, are we really having the wrong conversation here? And what impact does this have on the European Union and other jurisdictions? Have they addressed this issue? And what can we do? Because that just seems to be a different issue than disclosure, because this is publicly available stuff.

Mr. CEGLOWSKI. The power of inference, it does not come from the publicly available data. It comes from behavioral data, the incidental data, the observations about what did you click on, where were you at this time of day, who communicates with you. All of this digital exhaust that our lives produce that is collected then and tabulated. So it is only available to the very large tech oligopoly companies who can store it and can mine it.

Senator JONES. So going back real briefly—well, no, let me change directions a little bit and use some of that as well as this. What is to prevent or how can we prevent—there was a question a minute ago about discrimination, and I know all the laws. I mean, I follow them, I have practiced, and I tried to enforce them as a prosecutor and as a private lawyer. We have got laws about doing this. But as a practical matter, it still exists, and it exists every day. And in some instances, it is getting worse.

What can we do in this whole realm of data collection to try to ensure that people—whether it is businesses or whoever—do not collect this data and use it in a way that discriminates against Americans, or whatever, puts them in a protected class and then uses that data to discriminate? How can we prevent that? Anybody. Mr. Chase?

Mr. CHASE. We have laws on the books here in the United States now against discrimination in many, many respects. You do not necessarily need to see the inside of how the algorithm is working to look at the outcomes of decisionmaking. And often, I think probably many of the cases you were involved in, it was looking at the outcomes of the decisions that created the presumption, actually, that discrimination was going on.

Senator JONES. Yes, but looking at the outcomes is not the prevention. I mean, that is maybe a deterrent if you do some things. I am talking about trying to prevent discrimination to begin with.

Mr. CHASE. You know, I think the Europeans tried very hard not to stop artificial intelligence, AI, machine learning, all of these things. They were trying instead to much more narrowly focus on how you use profiling, whether or not there is automated decision-making, because some things you cannot stop. I would argue that humans are pretty biased in many respects, too, and so it is not just the agent. You really do have to look at what the outcome is.

Senator JONES. All right. Anybody else?

Mr. CLINE. Senator, some of the clients I am working with that are furthest ahead in their thinking on data ethics are putting in place some tools of processes. For example, policies and ethical impact assessments to identify—before they deploy a new machine learning or artificial intelligence capability, they will bring in a scientist, a mathematical scientist to look at the algorithm to identify if it could have disparate impact. So I am seeing some examples of tools that could address that.

Mr. CEGLOWSKI. I would just say that the bias is always in the data. The mathematical techniques that are being used are simple, they are well known. It is the data where the patterns live that they surface from. I think we need better visibility. I think we need strict limits on data retention. And we especially need research. We need access for people to be able to look and see what are the impacts of these algorithms, and nobody knows that. It is not just a question of people trying to do end runs around regulation. We genuinely are not familiar with how this will affect and impact society.

Senator JONES. All right. Thank you all.

The last thing I want to ask, how do we stop—how can we prevent a company, Facebook—Senator Kennedy talked about Facebook and not picking on Facebook. It could be anybody. And the end user agreements, and we have talked a lot about the disclosure. And I tend to agree with Senator Kennedy that my data is a basic property right that should be protected. But yet I have also got a lot of other rights that should be protected, like the right to a trial by jury that every day in this country somebody is buying a new car that has to give up that right in order to get that new car. Every day somebody gets employed, and they are having to give up a right to a trial by jury to go into arbitration.

My question is: How can we stop that? How can we stop Facebook or anyone else from saying if you want to get on Facebook, as are the billions of people around this world, you have got to give us your data and let it go? How do we stop that if they want to do that?

Mr. CEGLOWSKI. We pass laws.

Senator JONES. We have passed laws about a number of things, but if the Supreme Court will allow forced arbitration on things, there are always ways to get around the laws. Is there a way to adequately stop that from happening if you look at the historical precedent?

Mr. CEGLOWSKI. I am not able to answer that at this time.

Senator JONES. That is my biggest concern, that if we pass these laws and we do these things like that, then all of a sudden somebody will go around and big companies and big businesses will be able to do whatever the heck they want to do. So thank you.

Thank you, Mr. Chairman. Thank you, Ranking Member Brown. Chairman CRAPO. Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Mr. Chairman. Thank you all for your testimony. I have not been here for the whole hearing. I was at another hearing. So forgive me if I am plowing old ground.

But it seems to me as we look for what kind of structure or law we want to apply in the United States, we should look first to other countries that have implemented it, and so the GDPR is obviously something important to look at and see whether it is meeting its goals. We also have the California law.

So a very quick question to all of you, because we have had a lot of discussion about opt in/opt out. What has the experience been so far in Europe with this law, which is designed to give consumers rights? Are people exercising those rights, or are they deciding, look, I really need to use this system so much that I am going to opt in, not opt out? I am curious about your observations on how this law has been implemented so far and how it is working.

Mr. CHASE. Speaking more generally, it really is too soon to tell because some of the big cases that are coming through and a lot of the discussion has been about data brokers and decisions made by the—there have been complaints filed, but they have not been adjudicated. There has been guidance provided, but it is not yet there.

I think that there has been some belief that the data inventorying, the data hygiene practices that companies have undertaken has been useful in and of itself. There clearly has been a lot of increase in people's awareness of their data. Those parts are good. But at the same time, as I mentioned earlier, in part because of that, some of the mistrust of the internet has also gone up, and I think that that is natural.

Senator VAN HOLLEN. Are we finding people exercising their rights in terms of the choices they are given or not so much?

Mr. CLINE. Senator, I can tell you what I have seen operating in the day-to-day trenches. GDPR gives about eight rights to consumers, but when we look at the logs, the ones that are most exercised are the right to access, the right to erasure, and the right to opt out of marketing. These requests, though, are falling in an uneven way across the financial services industry. So those financial services companies that have the direct relationships with the consumers, like direct insurers or retail banking, they are feeling the most, perhaps sometimes thousands of those so far in the first year. Those in commercial banking or reinsurance on the back end sometimes may even have received less than 100 of these rights in the first year. So it is an uneven story so far 11½ months out.

Senator VAN HOLLEN. Got it.

Mr. CEGLOWSKI. I would say consumers are seeing a lot of benefit from the work being done internally to protect data. Part of finding out where data is in the system means making it safer. So I think there is a lot of internal reform that will have a long-term impact.

Europe is in the strange position of trying to regulate from across the Atlantic Ocean. The main tech companies are all here in the United States, and so we have seen them move lots of data out of the European Union. There is a lot of evasion of the GDPR that makes it harder to evaluate its impact.

Senator VAN HOLLEN. So, really quickly, are you all familiar with the California law?

Mr. CEGLOWSKI. Yes.

Senator VAN HOLLEN. So is there anything in the California law that is not in the GDPR that you think that we should look at as a positive thing or vice versa? Just to each of you, comparing the two, strengths and weaknesses, as we look to different models.

Mr. CEGLOWSKI. It is very hard to say with the GDPR because so many issues are still open to interpretation, especially around automated decisionmaking. I do not think that is in the California law, but I think that should be a strong focus. But it is hard to know what the decisions are going to be.

Mr. CLINE. When we look across the world's privacy laws and then compare those to California's new law, the one provision that does stand out is the prevention of—or the requirement for non-discrimination.

Senator VAN HOLLEN. OK.

Mr. CHASE. I do not know enough about California.

Senator VAN HOLLEN. Got it. All right. Thank you, Mr. Chairman. I appreciate it.

Chairman CRAPO. Thank you.

Senator SINEMA.

Senator SINEMA. Thank you, Mr. Chairman. And thank you to our witnesses for being here today.

Arizonans want to access the modern technological conveniences that make our financial lives easier, like online banking and apps for budgeting and for small finance. This technology helps Arizonans be more fiscally responsible in their everyday lives, plan and save for the future, and invest for retirement or help their kids go to college. But more than most, as Arizonans we value our privacy. Sometimes we just want to be left alone.

So I am committed to finding a thoughtful solution that protects fundamental privacy rights while ensuring continued access to the financial technology that makes life easier and better for Arizona families.

So with respect to privacy, it frustrates me that we still have not had a legislative response to the Equifax data breach. It affected nearly all of us, and yet Congress did actually nothing to tighten the Fair Credit Reporting Act and prevent another breach of our privacy.

Most people do not know that credit bureaus have a great deal of information about us, even before we apply for our first credit card or our student loan. We do not affirmatively consent to give that information. So I have a few questions about credit bureaus.

Mr. Ceglowski—did I say that correctly?

Mr. CEGLOWSKI. Close enough.

Senator SINEMA. Well, sorry. Thank you for being here. When examining the relationship between credit bureaus and consumers

under current U.S. law, would you say that consumers are more like the customer or more like the product?

Mr. CEGLOWSKI. With respect, I do not know enough about credit bureaus to be able to answer you.

Senator SINEMA. OK. So what challenges does this relationship pose for individuals who are dealing with identity theft or financial fraud? And what rights conferred under GDPR could be helpful to consumers here?

Mr. CEGLOWSKI. I think the Equifax lesson to everybody else is that there are no consequences to data breaches, that you can get by with impunity. I think that is a very dangerous lesson to send. The GDPR at least has quite long teeth that it can sink into offenders, and I think that would be desirable in any regulation here, to be able to actually punish these kind of blatant acts of either incompetence or just not caring about your customer.

Senator SINEMA. Thank you very much. You know, this issue matters a lot to me because of an Arizonan I know named Jill. Her daughter was a victim of synthetic identity theft, so this is the type of theft that occurs when criminals use a stolen Social Security number with little or no history on it to open bank accounts or credit cards under a new assumed name.

So the initial record is typically rejected, but once that denial occurs, a synthetic person is created, one that does not actually exist, and that synthetic person can be used to open up credit cards and other accounts, and they often rack up significant debt.

In 2011, someone did this to Jill's daughter, so last year we teamed up with Senator Scott of South Carolina and passed a bill called the "Protecting Children from Identity Theft Act." Our bill was signed into law last May, and so we are following its implementation. What our law does is strengthen the Social Security Administration's ID verification regime by modernizing it so it can be used for everyday financial transactions. We also called on SSA to cut through red tape that prevented Jill's family from getting a fresh start for their daughter.

So there is more to do because these kinds of financial crimes targeting our most vulnerable are becoming more prevalent with every data breach, and I hear from Arizonans every day about how they feel helpless and overwhelmed when it comes to protecting their privacy, safeguarding their finances. This is particularly true for seniors and those raising families. So we want to ensure that consumers have greater control of how their data is used and effective recourse should there be a breach.

So I would like to hear from all three of you: Do you think it is possible to keep our credit scoring system in the United States that has generally served us well over the years to make sure that Americans can get mortgages, buy cars, build their financial futures, but also advance some new commonsense reforms that protect people's privacy in a way that they are not currently protected?

Mr. CEGLOWSKI. Let me start by saying that many of the functions that credit reporting offered are now moving into the unregulated area of the online economy. So you are seeing Silicon Valley companies that have much bigger collections of personal data that are able to make decisions that have similar effect. For example, landlords now want to see people's Facebook accounts. These are

things that—I welcome strengthening the regulations around credit reporting. I think they should be extended in a similar spirit to where they are being practically applied in the same sense.

Mr. CHASE. Did you want to—

Mr. CLINE. Senator, I do not have personal experience in the credit reporting industry, but the companies I have served who have had the most success preventing data breaches and identity theft are those that conduct regular risk assessments and fix the vulnerabilities that they find.

Mr. CHASE. If I may, I wanted to mention earlier, but Equifax actually has paid a fine, at least one that I know of, but that was in the United Kingdom, 500,000 pounds, I believe. That was the maximum that was allowed under the old law. The data breach law in the General Data Protection Regulation could indicate a much higher fine. Also, there are other things that the regulator can do, including forbidding someone from doing data processing. That is point number one.

Point number two—

Senator SINEMA. Just to that first point, a fine is an important part of compensation, but what it does not do is increase privacy for consumers.

Mr. CHASE. I agree. The second thing, one of the points that you made in your opening remark, Senator, it would not be allowed under the GDPR for someone to say, “Here is a financial service”—you enter into a contract for a financial service—“and, oh, by the way, you have to sign this too because I want to be able to use all the data I can from you and use that separately.” It is interesting to me that some of the credit reference agencies are also agencies that are very much in the data brokering and reporting businesses. I find it interesting, although I am not sure—I think that there is a wall between the information.

Senator SINEMA. Thank you.

Thank you, Mr. Chair.

Chairman CRAPO. Thank you. And that concludes the questioning, except that Senator Brown and I would like to ask—Senator Brown will ask the question. We have a joint question.

Senator BROWN. And any of you can answer, but particularly if you would, Mr. Ceglowski. Your back-and-forth with Senator Jones was a bit unfulfilling because you were sort of talking in different ways. He was asking you to sort of take our profession for a minute and tell you what to do legislatively. Obviously, we do not expect legislative language from you. What should Congress do? How do you regulate without stifling innovation? Take as long as you want and just kind of give us—fairly briefly, but give us your thoughts on what we actually prescriptively should do.

Mr. CEGLOWSKI. Absolutely. So—

Senator BROWN. One more thing. I think that there is enough agreement here—you could see it from Senator Kennedy, you could see it from Senator Crapo’s and my comments that we really, unlike some issues that we have had greater differences on, this is something we can really do. So instruct us, if you would.

Mr. CEGLOWSKI. Absolutely. Well, I would say first that this seems to be a rare bipartisan opportunity where we can really kind

of speak with one voice about what should be done to improve things.

I mentioned before data retention and lifetimes on it. There is something deeply inhuman about saying that, something that you did haphazardly one day is going to be kept forever in a computer system that you do not have any visibility into. I think we need to bring humanity to how data is retained about—as one example, Google has now announced that they are going to allow people to delete location data after 3 or 18 months, proving that it is not really necessary to their business model to have this forever. I think that should be the default state of affairs, that things are forgotten unless you specifically ask for it to be remembered. You do not want Facebook deleting your wedding pictures, but you do want them deleting what your search queries were 7 years ago. Nobody needs to remember that.

I think there is an aspect in which we can have positive regulation where we create a legal basis for making credible commitments about privacy. So, for example, my company, I do not offer third-party tracking. I do not sell people's data. I would like to be able to promise that in a way that my customers can believe.

We had the example a few years ago of Snapchat. There was an application that showed—let you send videos that would disappear after you viewed them once. It turned out they did not really disappear. It turned out they were collecting all kinds of location data when they said they were not, and they got a slap on the wrist. If that slap on the wrist were much more than that, if people could go to jail for willful fraud, if people could face stiff fines, then we could compete on the basis of privacy, including small companies that can compete against the giants. So I think that is a second important way.

And then, finally, visibility. We have no visibility right now into what is being collected. Things like Facebook shadow profiles, if you are not a member of the site, what exactly do they know about you? What do they get from data brokers? How does the advertising economy work? All of these things are questions that we cannot regulate them until we have at least some sense of how they work under the hood. And I think one of the key steps toward visibility is this idea that if you are a user of a site, you should be able to get all of the information that that site has on you. You should be able to make that request like under the GDPR and receive an answer that is not 6,000 pages on a CD or whatever it is that people used to get from Facebook when they made this request, but something intelligible so that people can begin to understand what is being stored, and then we can start to have a conversation about how to limit that or how to make it—at least make its use safer.

Chairman CRAPO. Do either of the two of you want to respond?

Mr. CHASE. Just very quickly, I think that the United States has another particular to learn from Europe's experiences with the GDPR. So in this sense, maybe having the first mover advantage may not be the worst thing.

I think once again I will just reiterate that it is important to bear in mind what problem you are trying to solve. It is not all data and all uses and all functions. But that is what the GDPR covers. You need to be able to say, "What are you trying to do in this case?"

And I think that that goes for your mention of retention, that different—data can be used differently, and sometimes different retention requirements make a lot of sense. If you are talking about a social media platform, maybe it is different.

Finally, I think on the innovation part that you asked, Senator Brown, there are a lot of people who talk about the requirements of GDPR as putting a burden on small firms, that it is harder for them to comply. And I think that there is some truth to that. I think that there is also—in GDPR they have tried to make that less burdensome, but they also recognize that small firms, too, can have very sensitive data and can be a source of real grief for individuals if that data is out. So I think you have to regulate small firms, but I think that the enforcement thing that GDPR creates is much more risk-based; it is much more going toward companies that have lots of data and do lots of processing, and that makes a certain sense.

And, finally, Mr. Cline has mentioned a number of times the data protection impact assessments. There is a lot, I think, that can be looked at, learned from that.

Chairman CRAPO. Mr. Cline, did you want to add anything?

Mr. CLINE. A tool I have seen companies use to balance or to achieve both goals of consumer rights protection as well as encouraging innovation is the impact assessment. You know, the employees of the clients we serve all want to do the right thing, and when presented with competing goals, how do we innovate? How do we achieve the business purpose in a way that impacts privacy the least? These impact assessments document the rationale and the thinking and help get everybody on board toward competing goals.

Chairman CRAPO. Well, thank you. And, Mr. Ceglowski, your answer has prompted one more question to me, and I would just toss this out to see if any of you could briefly respond to it. When you mentioned the shadow files that in this case Facebook creates, those are files being created, I assume, without any connection with the individual whose data is being utilized, and the information has been collected elsewhere. If an individual knows that that data is being collected in that way, then I guess they could be given a right by the law to demand that that stop or be identified or made transparent. But it seems to me that that could be happening and is happening in many, many different circumstances and in different ways.

How does the individual know in order to opt out?

Mr. CEGLOWSKI. My understanding is that we simply do not have that right now, and we do not have the visibility. I might be wrong. I am not an expert.

Chairman CRAPO. Mr. Chase?

Mr. CHASE. I draw your attention to Article 14 of the GDPR, which I mentioned previously. There are obligations. For Facebook in that sense to do a synthetic personality on someone in Europe, they would essentially have to tell that person that they are doing it. And there are three specific times when they have to do it. If they are doing it internally and they are not doing anything with it, that is one thing. But if they start taking that information and providing it to third parties for advertising and direct marketing, then that would be problematic. But the article itself has fairly

detailed requirements about what needs to be notified to any individual when they are doing profiling businesses—profiling work on individuals without having gotten the information directly from the individual himself or herself.

Chairman CRAPO. Thank you. So does the GDPR require that any time a company sells an individual's data that the individual be notified that it is being utilized in that fashion?

Mr. CLINE. It requires their consent, so more than a notification.

Chairman CRAPO. All right. Thank you.

Again, I want to thank each of the witnesses for coming here and sharing your insights as well as your written testimony, which will be made a part of the record. As you can see, there is a lot of not only bipartisan but strong interest here in getting this issue resolved, and we appreciate—I suspect you will get some more questions from us, and to the Senators who wish to submit questions for the record, those questions are due to the Committee by Tuesday, May 14. And we ask each of the witnesses if you would respond to them as promptly as you can.

Again, we thank you for your efforts on our behalf to be here and to give us your insights, and this hearing is adjourned.

[Whereupon, at 11:51 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

On February 13, Senator Brown and I invited feedback from the public on the collection, use and protection of sensitive information by financial regulators and private companies in light of the immense growth and use of data for a multitude of purposes across the economy.

The Committee appreciates the insights and recommendations of respondents, who expressed a range of views on the topic of data collection, use and sharing and how individuals can be given more control over their data.

Building on that effort, today the Committee will take a closer look at the European Union's General Data Protection Regulation, or GDPR, and other approaches to data privacy, including the impact on the financial services industry and how companies collect and use information in marketing and decisionmaking related to credit, insurance or employment.

Providing testimony to the Committee today are three data privacy experts, including Peter Chase, Senior Fellow, The German Marshall Fund of the United States; Jay Cline, Privacy and Consumer Protection Leader, Principal, PwC US; and Maciej Ceglowski, Founder, Pinboard.

Each witness brings a unique perspective on the practical implications of implementing and complying with new data privacy laws; what has worked and what has not worked to give individuals more control over their data; and considerations for the Committee as it explores updates to Federal data privacy laws within the Banking Committee's jurisdiction.

My concerns about big data collection go back as far as the creation of the CFPB, which was collecting massive amounts of personal financial information without an individual's knowledge or consent.

In 2014, the GAO reported that the Bureau alone was collecting information on upwards of 25 to 75 million credit card accounts monthly, 11 million credit reports, 700,000 auto sales, 10.7 million consumers, co-signers and borrowers, 29 million active mortgages and 5.5 million private student loans.

Consumers deserve to know what type of information is being collected about them, what that information is being used for and how it is being shared.

Financial regulators are not the only ones engaged in big data collection; private companies are also collecting, processing, analyzing and sharing considerable data on individuals.

The data ecosystem is far more expansive, granular and informative than ever before.

As the U.S. economy becomes increasingly digital, people are using the internet, including search engines and social media, mobile applications and new technologies to manage and carry out more parts of their everyday lives.

The digitization of the economy allows for seamless access to both more generalized and granular pieces of data on individuals and groups of individuals, including data collected, with or without consent, directly from individuals, tangentially to individuals' activities, or gathered or purchased from unrelated third parties.

In particular, data brokers play a central role in gathering vast amounts of personal information—many times without ever interacting with individuals—from a wide range of public and private sources, which is then sold or shared with others.

In 2014, the Federal Trade Commission issued a report entitled, "Data Brokers: A Call for Transparency and Accountability," in which it highlighted data brokers' big role in the economy and concerns around their transparency and accountability.

In many cases, an individual's data or groups of individuals' data is used in ways that provide value, such as risk mitigation, fraud prevention, and identity verification, or to meet the requirements of laws or regulations.

However, in many other cases, that data can be used in ways that have big implications for their financial lives, including to market or make decisions on financial products or services that impact a consumer's access to or cost of credit and insurance products, or in ways that impact their employment prospects.

In any case, the way that an individual's or groups of individuals' data is used matters immensely.

As its rightful owner, an individual should have real control over his or her data.

A complete view of what data is collected, the sources of that data, how it is processed and for what purposes, and who it is being shared with is vital to individuals exercising their rights.

People should also be assured that their data will be reflected accurately, and have the opportunity to opt out of it being shared or sold for marketing and other purposes.

In 2016, the European Union took steps aimed at giving individuals more control when it replaced a 1995 Data Protection Directive with the General Data Protection Regulation, or GDPR.

The European Union's principals-based GDPR is broader in scope, applying to a more expansive set of companies, including some based in the United States, and more types of personal information than its previous Directive.

The GDPR also imposes specific responsibilities on both data controllers and data processors, and enumerates rights for individuals with respect to their personal information.

In contrast to the European Union, the United States has adopted Federal laws focused on data privacy within particular sectors.

Two such Federal laws in the Banking Committee's jurisdiction are the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act.

Today, I look forward to hearing more about the principles, obligations and rights underlying GDPR and how those differ from the previous 1995 Data Protection Directive; how GDPR addresses data brokers and other companies that collect and disseminate personal information, often without an individual's knowledge, and ways the Fair Credit Reporting Act may be adjusted to account for activities by such entities; challenges U.S. financial institutions have faced in implementing and complying with GDPR; how financial institutions' privacy practices have evolved since its enactment; and how individuals have responded to this additional information and rights with respect to their data; whether individuals actually have more control over their data as a result of GDPR, and what the European Union did right and wrong in GDPR; and considerations for the Banking Committee as it looks to update and make improvements to Federal laws within its jurisdiction.

Thanks to each of you for joining the Committee today to discuss GDPR, data privacy and individual rights.

PREPARED STATEMENT OF SENATOR SHERROD BROWN

I'm excited to be working in a bipartisan way with Chairman Crapo on protecting Americans' sensitive personal data—an issue everyone agrees is important.

As we start to think about this subject, I hope we do it with an open mind. Technology has advanced rapidly, and we should have some humility to admit that we don't even know all there is to know about what happens when personal information is collected on a large scale. As it turns out, personal information can be far more than your name, address and Social Security number. Sometimes harmless data, once it becomes big data, can reveal big secrets.

Take for example a fitness tracking app that became popular among U.S. soldiers stationed abroad. Many of those servicewomen and servicemen tracked their daily workouts, and when the aggregated fitness tracking information became public, heatmaps of common running paths revealed the locations of secure military facilities all over the world.

Even when we agree that data is sensitive, we're often not good at protecting it.

Most of us still remember the Equifax breach that exposed the detailed financial information of more than half the U.S. adult population—information that will remain useful to potential criminals for the rest of those 147 million Americans' lives.

The Equifax case also reminds us that we can't fix this by just warning people they should share less personal data on the internet. People weren't putting their Social Security numbers on Facebook—Equifax had collected data from various sources, and in many cases people weren't even aware Equifax ever knew anything about them.

There's a lot of data floating around that can be compiled and analyzed in creative ways to make shockingly accurate predictions about our lives.

What you think of as your "personal data" isn't limited to bank passwords and credit scores.

As we learned several years ago, even if you don't have a Facebook account, Facebook builds a shadow profile of your activities, interests, and preferences from digital breadcrumbs spread by your friends and associates online.

Sometimes you may not realize that data is being monetized. Remember Pokemon Go? Did you know that businesses can pay to have Pokemon show up near them in the game, herding customers into their stores?

There's a common saying that "if you're not paying for the product, then you are the product." Services that appear free make money from your personal data.

It's not easy for consumers to protect themselves. "Buyer beware" is not a helpful warning, since most people cannot afford to protect themselves by opting out of

internet services just like they cannot opt out of banking products with arbitration clauses in them.

In today's world, telling people to look out for themselves when it comes to protecting their personal data is about as useful as telling people to look out for themselves when it comes to food safety.

We can't tell people to avoid the internet and avoid having their data collected any more than we can tell people to stop eating dinner. We can't abandon the people we serve when it comes to protecting them.

If we don't take this seriously, a handful of big tech corporations and financial firms will continue to strongarm customers into sharing their most intimate details.

So in addition to talking about ownership and control of our data today, I hope we can also talk about where Government needs to step in and create rules around the appropriate uses of personal data—regardless of whether a customer opts in. And I hope we can talk about what kind of data should or should not be collected, and for how long it should be stored.

This problem isn't just important to our personal privacy and our economy—it's also critical to our democracy. As the Cambridge Analytica scandal demonstrated, a big enough pile of seemingly meaningless data can give a bad actor ways to meddle in our elections.

The Banking Committee is only responsible for one slice of the data ecosystem—I hope to work with the Chairman of the Banking Committee as well as the Chairs and Ranking Members of the other committees of jurisdiction to set some common-sense rules on the use of Americans' sensitive personal data.

Thank you.

**Perspectives on the
General Data Protection Regulation
Of the European Union**

Prepared Remarks of

Peter H. Chase
Senior Fellow
German Marshall Fund of the United States

To the Hearing on

“Privacy Rights and Data Collection in a Digital Economy”

Before the

**Committee on Banking, Housing and Urban Affairs
Of the United States Senate**

May 7, 2019

Chairman Crapo, Senator Brown, Members of the Committee:

Good morning and thank you for providing me the opportunity to offer some perspectives on the European Union’s General Data Protection Regulation (GDPR), as the Committee considers whether and how the United States should adopt a comprehensive data protection law.

My name is Peter Chase; I am a Senior Fellow at the German Marshall Fund of the United States, a 501(c)(3) nonpartisan and not-for-profit organization based in Washington, D.C. GMF was established in 1972 by a gift from the German government to recognize the 25th anniversary of the Marshall Plan to rebuild Europe after World War II, and is dedicated to promoting transatlantic cooperation in the spirit of that Plan. The views I express are mine alone. I am not speaking for the German Marshall Fund of the United States, which does not take institutional positions on policy issues.

My perspectives on the GDPR are based on nearly a quarter-century of work on economic relations between the United States and the European Union (EU), first as part of my 30-year career as a U.S. Foreign Service Officer,¹ then when representing the US Chamber of Commerce in Europe from 2010 to 2016, and now with GMF. My primary interest in the EU’s data protection regime has been on the provisions concerning transfers of personal information to

¹ I was assigned to the U.S. Mission to the European Union in 1992, when the EU was considering the GDPR’s predecessor, the Data Protection Directive. I continued to work on the issue when I served in the U.S. Embassy to London and as the Chief of Staff to the Under Secretary for Economic Affairs as the U.S. and EU were negotiating the Safe Harbor Agreement, and ran again into data protection issues again when assigned to the U.S. Mission to the European Union in 2007-2010.

third countries like the United States, in the law enforcement and national security context as well as for the private sector, although I of course have been concerned with the other aspects of that regime as well. In this context, I will try to provide an objective description and assessment of the GDPR. I will note my personal views and opinions when offering those.

My comments will cover three aspects of the GDPR:

- its antecedents and political context;
- its provisions; and
- its implementation.

The European Union

But first, a word on the European Union, as the GDPR in many respects reflects the evolution and structure of the EU. The European Union stems from a series of international treaties concluded in 1957 initially among six countries, a number that progressively increased to 28 today. The underlying ethos of the treaties is that closer integration can prevent Europe from being engulfed again by the conflagration of war. In acceding to the EU, countries take the sovereign decision to promote that integration by jointly making laws that apply in each of their territories.

In this structure, all law and regulation must first be proposed by the **European Commission**, which is intentionally independent of any member state, but these proposals only gain legal effect if adopted by the **EU Council**, representing the sitting governments of the member states, and the **European Parliament**, directly elected representatives of the population in each member state. (The Council is often likened to the U.S. Senate, and the European Parliament to the House of Representatives; indeed a process akin to our conference committees is needed for the two to agree on a single final text.) EU laws generally take two forms – **Directives** that member states implement through national law, and **Regulations** that have direct effect. The European Court of Justice (ECJ), like our Supreme Court, ensures that laws, both at the EU and national levels, are consistent with the underlying EU Treaties.

GDPR's Antecedents and Political Context

The immediate predecessor to the General Data Protection Regulation was the Data Protection Directive, adopted in 1995 on the basis of a proposal originally submitted by the Commission in 1990. At the time of the proposal, establishing a Single Market among the then 12 members² of the European Economic Community (as it was then known) was the top priority. The Commission argued that seven member states³ had adopted national data protection laws, and that this “*diversity of national approaches and the lack of a system of protection at the Community level are an obstacle to the completion of the Single Market ... (such that) the cross-border flow of data might be impeded just when it is becoming essential to the activities of*

² Denmark, Ireland and the United Kingdom having joined Belgium, France, Germany, Italy, Luxembourg and the Netherlands in 1973, while Greece joined in 1981 and Spain and Portugal in 1986.

³ Denmark, France, Germany, Ireland, Luxembourg, the Netherlands, the United Kingdom.

*business enterprises and research communities*⁴ At the time the European Economic Community did not cover fundamental rights of individuals, but the Commission asserted the importance of these as expressed in the European Convention on Human Rights under the Council of Europe (a separate international organization). Indeed, it harkens back to the 1981 *Council of Europe Convention 108 for the Protection of Individuals with Regard to the Automated Processing of Personal Data* (pursuant to the ECHR protection of privacy) as well as the 1980 *OECD Guidelines on the Protection of Privacy and the Cross-Border Flow of Personal Data* as both the ethical and intellectual foundations for the high level of protections of personal data that the Proposal recommends. (It also calls for the Community itself as well as the five member states that had not acceded to Convention 108 to do so.)

While many of the specific provisions of the 1990 Commission proposal for the Data Protection Directive are reflected in the version as eventually adopted in 1995, the political context changed significantly in the meantime, including through the 1993 entry into force of the Maastricht Treaty. This created the construct of the European Union as a “roof” over the European Community, complemented by two new “pillars” of *intergovernmental* cooperation among the member states in the areas of law enforcement and foreign policy.

The Maastricht Treaty also strengthened the role of the European Parliament in law making, which arguably increased the Directive’s emphasis on protecting personal data as a fundamental right. This increased emphasis, however, also reflects the political significance of the fall of the Berlin Wall, the collapse of the authoritarian regimes of the Warsaw Pact countries and the reunification of Germany (which brought additional members to the European Parliament), as well as the expansion of the EU to include Austria, Finland and Sweden in 1994.

It is often said that the importance of data protection as a fundamental right reflects Europeans’ sensitivity about government spying, especially under the Stasi and the Communist governments in Central Europe. This is true, in part. But the 1995 Data Protection Directive applies primarily to commercial processing of data, and to that of the governments in the “normal” course of their business; law enforcement and intelligence functions are explicitly outside the scope. And indeed, my recollection of the debate during that time was that much of the concern was more about direct mail advertising and spam, rather than civil liberties.

The political context changed dramatically between the 1995 adoption of the Data Protection Directive and the adoption, in 2016, of the General Data Protection Regulation. I will highlight some of the key differences in the provisions between the two below, but here the critical contextual changes include:

- the conclusion of the Charter of Fundamental Rights and Freedoms of the European Union in 2000; although not at that time a legal text of the European Community, the Charter brought a fundamental right to privacy and to data protection into the general legal regime of the Community as all the EU institutions pledged to respect it;

⁴ Commission of the European Communities, [Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security](#), COM(90) 314, 13 September 1990, page 4.

- the accession into the EU of virtually all of the former Warsaw Pact countries in 2004⁵ and 2007;⁶
- the entry into force of the Lisbon Treaty in November 2009, which inter alia:
 - gave the European Union legal personality;
 - integrated the law enforcement and foreign policy pillars into the EU structure (as opposed to having the Commission support inter-governmental cooperation); and
 - formally incorporated the EU Charter of Fundamental Rights into the EU Treaty.⁷

Thus, while the 2012 Commission proposal for a General Data Protection Regulation to update the 1995 Data Protection Directive talks about both the huge evolution in technology in the intervening 17 years as well as the frictions created in the Single Market by the many national laws that were required to implement the Directive, that proposal placed a much greater emphasis than the 1990 proposal on the importance of individual's fundamental right to privacy and to control the use of personally identifiable information.

This then snowballed with the Snowden revelations in 2013 of US government access to data held by major American IT firms, which among other things led the Commission, the much enlarged and varied European Parliament, and all the bodies entrusted with interpreting and enforcing the Data Protection Directive to significantly strengthen all the protections that the Regulation provided.

The General Data Protection Regulation

Whereas the 1995 Data Protection Directive has 34 Articles and is 19 pages long, the General Data Protection Regulation (hereafter GDPR) has 99 Articles and is 88 pages long (with very small print!).

Direct Effect, "Pre-emption"

The most important legal difference between the two is that GDPR is a Regulation, having direct legal effect in the territories of all 28 EU member states as of May 25, 2018. In providing this uniform direct effect, GDPR eliminates obstructions to data flows (potentially) caused by divergences in national law, thus "ensuring" the primary objective of allowing the free flow of personal data within the European Union. In that sense it "pre-empts" all existing national data protection laws, although it provides some instances where the member states either may or must adopt certain accompanying legal measures (e.g., to strengthen the powers of the national Data Protection authorities).

Expansive Scope

Like the Data Protection Directive, the GDPR is an **omnibus bill** covering virtually all "processing" by both government and non-government entities of **personally identifiable**

⁵ The Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Slovakia, Slovenia.

⁶ Bulgaria and Romania.

⁷ Although, in so doing, explicitly not expanding the European Union's powers beyond those actually in the EU Treaties.

information (PII), where PII is expansively defined as “any information related to an identified *or identifiable* natural person” (including online identifiers like an IP address), and where “processing” means “any operation performed on personal data, *whether or not by automated means*.” Not covered is processing by governments that does not fall within the scope of the EU Treaties or is related to national security or law enforcement, as well as that done by individuals for purely personal reasons.

Processing of any PII of anyone in the world done in the territory of the EU is of course covered, but so too is that done by anyone *outside* the EU if that processing:

- includes information of residents in the EU and is done on behalf someone in the EU (who is then responsible for how it is processed); or
- is done either to offer goods and/or services to someone in the EU (that is, for a commercial reason) or to “monitor behavior” of a person where that behavior takes place in the EU.

With this hugely expansive scope, GDPR then lays out:

- Principles related to the processing of personal information;
- Rights of individuals whose data is processed;
- Obligations on “controllers” of PII doing the processing (as well as “processors” who process data on behalf of the controllers);
- Restrictions on the transfer of PII outside the European Union; and
- A series of administrative and enforcement measures.

The most important aspects of each of these parts are described briefly below, with a bit of additional detail on three of the most critical (consent and the other legal bases for processing, profiling and automated decision-making) discussed in the third section on implementation.

Data Processing Principles

GDPR specifies that anyone that has and processes personal data is accountable for ensuring that such data is:

- Processed in a legal, fair and transparent fashion (lawfulness);
- Collected and used only for specified, explicit and legitimate purposes (purpose limitation);
- Limited only to what is necessary for the specific purpose of processing (data minimization);
- Accurate, with inaccurate data rectified and erased (data accuracy);
- Retained only as long as needed (data retention); and
- Protected (integrity and confidentiality).

There are six legal grounds for processing personal information under the “lawfulness” principle, determined by whether the controller:

- has the consent of the individual (“freely given, specific, informed and unambiguous”); OR
- needs to do it to perform a contract with that individual; OR
- must comply with a legal obligation spelled out in law; OR
- believes so doing is in the “vital interests” of the individual or another person; OR

-- will do so for a public purpose, again spelled out in law; OR
 -- can demonstrate that so doing is in the "legitimate interests" of the controller or a third party, as long as such interests are not over-ridden by those of the individual.

The processing of "special categories" of personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic and biometric information, health or sexual orientation) is **prohibited**, *unless*:³

- The individual provides explicit consent (stronger than informed consent);
- the information is already "manifestly made public" by the individual;
- the processing is necessary related to employment or social security;
- the processing is done by a foundation, political, trade union or other non-profit body for the purposes of that body; or
- there is a substantial public, scientific, medical or research reason to do so.

Rights of the Individual

GDPR's Third Chapter empowers individuals to ensure they:

- Understand what PII is being collected, by whom, for what specific purpose and on what legal grounds, who will have access to it (whether a processor, or a third party, including if overseas), and how long it will be retained; *this applies whether the data is collected directly from the individual or not*;
- Can access their PII held by a controller;
- Can rectify the data so held, and demand its restricted use or erasure ("right to be forgotten") when it is no longer needed, the individual has withdrawn consent, the processing is done without a legitimate basis, or the individual objects to the processing, although the exercise of these rights cannot interfere with others' right to freedom of expression and information, compliance with a legal obligation, public health needs, or legal claims;
- Can receive and transfer this data to another controller ("portability");
- Can object to any processing based on the "legitimate needs" grounds noted above, and particularly to processing for direct marketing, and profiling related to that; and
- Are not subject to a "decision based solely on automated processing (including profiling) ... which produces legal effects or similarly significantly affects him or her."

EU or member states can restrict these rights for a number of reasons (national security, law enforcement, etc.) but the laws must clearly spell out why such restriction is necessary.

³ The ten exceptions in Article 9(2) from processing sensitive data are more detailed than presented here.

Obligations on the Controller/Processor

Any “controller” that has personally identified information (or a “processor” working on that data on behalf of the controller) is legally responsible for implementing “appropriate technical and organizational measures” to ensure that the principles and individual rights spelled out above can be effected. In particular, they must:

- ensure they have a specific legal grounds for any processing;
- provide users clear and easily understandable information about the data they will collect, how it will be used and the specific legal grounds on which it will be processed, who will have access to it, etc.;
- grant access to and copies of any PII they hold on request, and comply with withdrawals of consent, requests for amendment, and restrictions on or objections to processing (with the exceptions noted above);
- use technical means such as “pseudonymization,” encryption and data protection by design/default to ensure data minimization;
- conduct “data protection impact assessments” prior to any new processing that may involve high risks to individuals’ rights (including profiling and automated decision-making), in consultation with the appropriate national data supervisor;
- keep records related to their data processing;
- provide appropriate security/protection for the data, notifying supervisory authorities (and if appropriate, individuals) of data breaches; and
- appoint a data protection officer, if they are a public authority, regularly process large amounts of PII, or deal in large amounts of personal data. Otherwise, firms should be able to access a data protection officer through, for instance, their industrial association.

Adherence to Codes of Conduct or other certification schemes can be used to help demonstrate compliance.

Controllers or processors not established in the Union must have a representative in the EU to ensure they can be held legally accountable, although this does not apply if they are a public authority or their processing is “occasional” and doesn’t include large amounts of sensitive data.

Third Country Transfers

Transfers of personal data out of the EU should in principle “take place *only* if” (“prohibited” is the word used in Recital 107) the “level of protection of natural persons guaranteed by this Regulation is not undermined.” In particular, transfers can take place if:

- the Commission deems a country provides an “adequate” level of protection (which it has done for six countries outside Europe, most recently Japan, as well as for U.S. firms that adhere to the U.S.-EU “Privacy Shield” arrangement);
- appropriate safeguards exist in the form of contract clauses, binding corporate rules, adherence to Codes of Conduct or certification schemes;
- the individual has given *explicit* consent to the transfer;
- the transfer is necessary for performance of a contract or in the public interest, etc.

Otherwise, transfers may only take place where it is not repetitive, does not involve many individuals, is in the “legitimate interest” of the controller (to the extent that the individual’s interests don’t override those), AND where the controller has assessed the risks associated with the transfer, established appropriate safeguards and informed individuals of the risks involved.

Implementation and Enforcement

Chapters 6, 7 and 8 of the GDPR go to its administration and enforcement. As noted above, a primary objective of the GDPR is to ensure the free flow of data within the EU and the consistent application of the law through a Regulation that has direct effect in the territories of each member state. To that end, one of the novel aspects of the Regulation is the notion of a “lead” supervisory authority that oversees and regulates the activities of companies operating in a number of member states. The GDPR accordingly strengthens the roles, responsibilities, powers (including investigatory and “corrective”) and independence of the member state data protection authorities (many of which have been upgraded to Commissions). It further establishes a European Data Protection Board (EDPB) in which they are all represented and which is designed to facilitate cooperation among them, adjudicate differences between them, and issue guidance interpreting the GDPR which they will apply to the controllers and processors in their territory.

These national data protection supervisors have the authority to issue warnings and reprimands, order compliance with an individual’s requests, impose temporary or definitive bans on processing, order restrictions or erasure of data, order suspension of data flows and impose administrative fines, which can be up to €20 million or 4 percent of total worldwide annual turnover (whichever is larger) of a “controller.” Decisions of the data protection authorities are subject to judicial review.

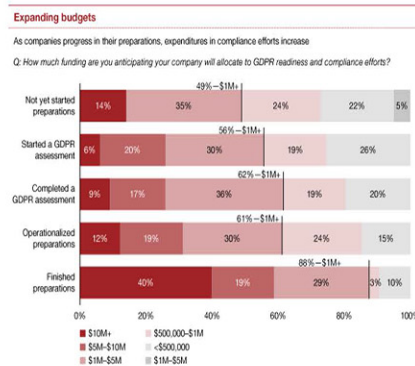
GDPR Implementation

The GDPR has been in effect for almost a year, with varying claims about its impact, stringency, efficacy, workability and enforcement.

According to a number of reports, companies – including American firms – have spent literally billions of dollars over the past two years to bring themselves into compliance.⁹ Another often-quoted 2018 survey by PwC¹⁰ notes, inter alia, that the more advanced a firm is in its compliance efforts, the greater (and more certain) the budget for compliance is, with over 40% of compliant U.S. companies saying they spent over \$10 million each:

⁹ Oliver Smith, [The GDPR Racket: Who’s Making Money from this \\$9 billion Business Shakedown](#), Forbes, May 2, 2018.

¹⁰ [Pulse Survey: GDPR Compliance Budget Top \\$10 million for 40% of Surveyed Companies](#), PwC



And the International Association of Privacy Professionals, perhaps gleefully, once estimated that some 75,000 Data Protection Officers would be needed worldwide to ensure compliance.¹¹

Most of this “investment” of course stems from firms’ concern about the potentially enormous cost of *not* complying – if the maximum fine of 4% of global sales is applied. Especially in large U.S. and European companies, where lawyers abound and compliance departments have serious clout, not complying with the strictest interpretation of the law as written is not an option. That said, the largest enforcement action to date, at least in terms of penalties, was a €50 million fine imposed on Google by the French data protection authority in January 2019 largely for lack of transparency related to the use of information from its Android system on phones in France. But a small Austrian business was fined in October for the overly broad use of its security cameras, a German social media firm paid €20,000 for poor practices related to a data breach, and a data processor in Poland was fined €220,000 for data scraping and direct mailing about which consumers complained.¹²

And in fact, thus far, most national data protection authorities are focusing on helping and advising local firms on implementing the GDPR and adopting “good” data processing practices. As such, most of the thousands of enforcement “actions” that have occurred over the last ten months have involved amicable resolutions, warnings and advisory steps.¹³

¹¹ Rita Heimes and Sam Pfeifle, [Study: GDPR’s Global Reach to Require at Least 75,000 DPOs Worldwide](#), IAPP, November 9, 2016.

¹² Steven Pinson, [The Need for United States and Canadian Businesses to have a GDPR Compliance Initiative in Place is Paramount](#), Mondaq, February 1, 2019 (accessed April 30, 2019).

¹³ See, for instance, Data Protection Commission of Ireland, [Annual Report \(May 25, 2019–December 31, 2019\)](#), 28 February 2019, which notes that it had received 2,864 formally-recognized “complaints” since GDPR entered into effect (and an additional 612 prior to May 25), of which 868 had been concluded (usually amicably, but leading to 32 formal decisions, 13 in favor of the complainant), 510 had proceeded to complaint-handling and 550 were being actively assessed; of the complaints, 136 were by other EU member state data protection authorities to the Irish DPA as the lead supervisory authority for multinational firms based in Ireland.

In this sense, some of the warnings about the negative effects of the GDPR have been overblown. GDPR itself is very prescriptive, and the right of every individual to ask a company for information about the data it holds on him or her, and to file a complaint, undoubtedly implies a lot of additional work (and cost). But very few data processing activities – including profiling for direct-marketing/advertising purposes -- are actually prohibited, although they can no longer be undertaken with impunity. And while Data Protection Authorities must respond to all complaints, they have discretion about how to handle them. Further, while GDPR may not be directed solely toward addressing identified *tangible* “harms,” it is risk-based and emphasizes situations that involve processing of large amounts of personal data (especially if that processing includes sensitive information) from large numbers of individuals.¹⁴ Bigger companies, especially in the IT sector (but also many others, including auto and energy companies), are accordingly much more likely to be watched. Knowing this, many such companies have spent the last two years carefully scrutinizing their own data collection, use and retention policies, a “data hygiene” process that some now welcome (albeit usually in hind-sight).

GDPR Guidance

Indeed, in some respects the most important implementation steps that have happened are the guidance documents issued by the newly-constituted European Data Protection Board, the successor of the so-called Working Party 29 (WP-29) that was established under Article 29 of the previous Data Protection Directive. Some of these guidance documents are interpretations by the WP-29 of the GDPR following its adoption but prior to its entry into force in May 2018, which are largely on issues where the GDPR and its predecessor are similar. Since, the EDPB has either adopted many of these WP-29 documents (giving them more force than they had under the old law) or issued its own documents for public comment and then as final “rulings.”

These guidance documents go to some of the most controversial provisions of the GDPR, including the notions of consent and contracts as legal bases for processing, and about profiling, automated decision-making and “artificial intelligence,” all discussed further below.

Consent: The guidance on consent¹⁵ helps clarify the issue of lawful processing in part as it underscores (repeatedly) that informed and unambiguous consent is *only one* of the bases for processing, and indeed that it often is *not* the best one. Among other things, it stresses that “inviting people to accept a data processing operation should be subject to rigorous requirements, since ... the controller wishes to engage in a processing operation that would not be legal without the data subject's consent.” It further specifies that controllers cannot “bundle” consent permissions; individuals must consent to each specific processing use of their data at a “granular” level, and must have the right to withdraw their consent from each specific use without that affecting their enjoyment of the other aspects of the offering, especially when the collection or processing of the PII is not strictly necessary for the performance of the contract (although it might be useful for advertising purposes). (For instance, a bank cannot ask for PII to

¹⁴ This is most obvious in the requirements behind the need for a “Data Protection Impact Assessment,” see, e.g., Irish Data Protection Authority, [List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment](#), 15 November 2018.

¹⁵ Article 29 Working Party, [Guidelines on Consent under Regulation 2016/679, adopted on November 28, 2017, as last Revised and Adopted on 10 April 2018](#).

be used for direct marketing purposes in connection with the opening of a bank account.) Given the “imbalance of power,” governments/public authorities and employers should never rely on consent, as it cannot be freely given in these contexts. Further, getting consent must be matched by an equally easy-to-do withdrawal of that consent, subjecting controllers to possible requirements to delete PII they may have.

Contracts: But while this WP-29/EDPB interpretation of the limitations on personal consent may “nudge” controllers to other legal bases for processing, those too are strictly interpreted. A draft Guidance document¹⁶ the EDPB has published for three months of public comment on the use of a contract as a legal basis for processing, for instance, notes that while a contract is essential for the conduct of most business relations (including for the conduct of information society services funded through advertising), the principles of purpose limitation and data minimization apply. The EDPB notes, for instance, that where processing is not *in fact objectively necessary* for the provision of the service, other processing (for instance, for direct marketing purposes) can take place only if it relies on another appropriate legal basis (about which the user must be informed). As the Guidance document explains through example:

Example 1

A data subject buys items from an on-line retailer. The data subject wants to pay by credit card and for the products to be delivered at home. In order to fulfil the contract, the retailer must process the data subject’s credit card information and billing address for payment purposes and the data subject’s home address for delivery. Thus, Article 6(1)(b) [processing under a contract] is applicable as a legal basis for these processing activities. However, if the customer has opted for shipment to a pick-up point, the processing of the data subject’s home address is no longer necessary for the performance of the purchase contract and thus a different legal basis than Article 6(1)(b) is required.

Example 2

The same on-line retailer wishes to build profiles of the user’s tastes and lifestyle choices based on their visits to the website. Completion of the purchase contract is not dependent upon building such profiles. Even if profiling is specifically mentioned in the contract, this fact alone does not make it ‘necessary’ for the performance of the contract. If the on-line retailer wants to carry out such profiling, it needs to rely on a different legal basis.

Automated Decision-Making/Profiling: This sort of very specific, legalistic and protective interpretation of the GDPR (“Data subjects can agree to processing their personal data, but may not trade away their fundamental rights”¹⁷) is reflected as well in the EDPB’s Guidance document on automated decision-making and profiling,¹⁸ which says that:

“... profiling and automated decision making can pose significant risks for individuals’ rights and freedoms which require appropriate safeguards. These processes can be

¹⁶ European Data Protection Board, [Guidelines 2/2019, on the processing of personal data of Article 6\(1\)\(b\) GDPR in the context of the provision of online services to data Subjects, version for public consultation](#), April 9, 2019.

¹⁷ *Ibid.*, page 13

¹⁸ European Data Protection Board, [Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679](#), Adopted on 3 October 2017 as last revised and adopted on 6 February 2018.

opaque. Individuals may not know that they are being profiled or understand what is involved. Profiling can perpetrate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences.... In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustifiable discrimination.”

The document distinguishes between profiling and automated decision making, although it notes that the former is often a component of the latter. It is also careful to indicate that profiling often comes from the melding of personally identifiable information both provided by the individual *as well as obtained from other sources* to make inferences about likely future behavior, noting how the obligations of transparency and purpose limitation, including on further processing, figure into this. While it does not prohibit either of these processes per se, it holds them to a very high standard, and repeatedly notes the individual’s right to object in particular to their use for direct marketing purposes: “It also suggests it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering.”¹⁹

Artificial Intelligence: The GDPR provisions on automated decision-making and profiling are those most frequently related to “artificial intelligence” (AI, which is not explicitly addressed in the GDPR), as the term “AI” today is frequently used to refer to big data analytics, which often will involve personal information.²⁰ But European officials argue that these concepts should not be conflated: big data analytics, even that involving PII, is not the same as automated decision-making (defined as a decision about an individual produced “*solely* by automated means”). A controller wanting to engage in big data analytics involving (large amounts of) PII could do so, but only after conducting a Data Protection Impact Assessment to ensure that s/he has an appropriate legal basis to do so and that the rights and freedoms of individuals are not infringed. But where such processing leads to a decision with a significant impact on an individual, the individual has the right to ask for review of that decision by a human.

Conclusion

The EU’s General Data Protection Regulation stems from both a need for the European Union to prevent member states from having different regulations that obstruct integration (and cross-border trade in services) by having different data protection norms, as well as a deep belief in the fundamental right to privacy as exercised through an individual’s control over the use of data personally identified with him or her.

Europeans argue that a single universal approach to data protection is more effective than a sectoral one, that may only cover certain types of institutions rather than the underlying data that is to be protected, and that organizations outside the sector can abuse.

¹⁹ Ibid, page 15.

²⁰ See, for instance, the excellent discussion of the potential chilling effects of European use of AI in Nick Wallace and Daniel Castro, [The Impact of the EU’s New Data Protection Regulation on AI](#), Information Technology and Innovation Foundation (itif), March 27, 2018.

However, in adopting a prescriptive approach to data protection, the EU often assumes, rather than documents, societal harms that its legislation is meant to address. To some extent, EU officials appear to understand that GDPR may be overly restrictive, especially when it comes to the potential societal benefits of big data analytics to masses of personal data; they appear in conversations to be trying to offset this by expanding in some ways the “legitimate interests” of the controller to allow for this.

This, as well as the GDPR provisions on direct marketing, suggest that to some extent the “real” issue the GDPR (as with the Data Protection Directive) is meant to address is the monetization of personal data, where monetization is now meant broadly to include not just advertising, but also benefits from politically-directed micro-targeting of messages.

The GDPR principles, rights and obligations may provide useful guidance for U.S. law-makers as they consider whether the U.S. should adopt analogous legislation. But the specificities of the EU evolution and context should be borne in mind, as should the difficulties the EU addresses as it implements the Regulation. This is one of those instances where the United States, while not having the first mover advantage, may also benefit from moving second.

PREPARED STATEMENT OF JAY CLINE

PRINCIPAL AND U.S. PRIVACY AND CONSUMER PROTECTION LEADER,
PRICEWATERHOUSECOOPERS LLP (PwC)

MAY 7, 2019

Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee, I appreciate the opportunity to appear today as the Committee considers privacy rights and data collection in a digital economy. I am currently a Principal and the U.S. Privacy and Consumer Protection Leader at PricewaterhouseCoopers LLP (PwC). I am appearing on my own behalf and not on behalf of PwC or any client. The views I express are my own.

Lessons learned from U.S. financial institutions' GDPR experience, 2016–2019

My testimony today will examine the experience of U.S. financial institutions (FIs) with the European Union (EU) General Data Protection Regulation (GDPR). It is an experience marked by large-scale technical and organizational change to afford new privacy rights to EU residents in an evolving regulatory environment. It is my hope that my testimony will be useful to the Committee as it considers the collection, use, and protection of personally identifiable information by financial regulators and private companies.

GDPR caused many U.S. FIs operating in Europe to undertake their largest-scale privacy program initiatives in two decades. Beginning after the ratification of the GDPR in April 2016 and generally accelerating a year later, these initiatives often rivaled the scale of U.S. FIs' earlier mobilizations to prepare for the Privacy Rule of the Gramm-Leach-Bliley Act (GLBA) and other related U.S. data privacy laws and regulations. As a result, U.S. FIs generally used all of the GDPR's 2-year grace period to prepare for the law's "go live" date in May 2018.

Impact of GDPR requirements on U.S. FIs

The GDPR introduced several new obligations on U.S. FIs.

- *New requirements on data-subject rights* most affected retail banks and direct insurers—because of their direct exposure to fulfilling data-subject requests (DSRs)—and least affected commercial banks, re-insurers, payment-card companies, and asset-management companies that generally had indirect exposure to DSRs.
- *New requirements on data privacy program accountability* by comparison most affected larger, diversified groups of companies that had to allocate more resources to accommodate their business variations and least affected more homogenous FIs.

The effects of the GDPR requirements included increases in headcount, changes in information systems, and alterations in products and services.

The GDPR also introduced several new organizing principles to U.S. FIs. Concepts such as "personal" data including data indirectly identifiable to individuals, "sensitive" personal data, "pseudonymized" data, "high-risk" data processing, "large-scale" data processing, "original purpose" of data collection, "cross-border" data transfer, "data controller," and "data processor" materially affected the policy regimes of all U.S. FIs operating in the European Union. The GDPR also introduced a new enforcement environment for U.S. FIs. This environment resulted in new and uncertain risk exposures. In the United States, for example, class-action lawsuits related to the Telephone Consumer Privacy Act (TCPA) are a significant driver of data privacy-related economic risk for U.S. FIs. The private right of action for GDPR-related issues, however, is a new and untested citizen-led enforcement channel in the European Union that could have broader impact than the TCPA because of the broader scope of covered data. Moreover, the new powers of EU data-protection authorities (DPAs) to impose fines of up to 4 percent of annual global revenues has expanded the potential risk exposure of the largest corporations into the billion-dollar range for the first time. Similarly, the EU DPAs' power to issue injunctions to stop data processing that runs counter to the GDPR could have the result of ending revenue-generating commercial activities that depend on that data processing. As the GDPR and its enforcement regime influence how other jurisdictions in the United States and around the world take their next steps on data privacy law and enforcement, U.S. FIs operating globally are re-evaluating their approaches to privacy-risk management.

Challenges, insights, and questions

The U.S. FI experience with addressing the GDPR can be grouped into three categories: top challenges, implementation insights, and unanswered questions.

Seven GDPR implementation challenges for U.S. FIs

Financial institutions use personal data to provide most of their products and services. Whether to set up a bank or investment account, install a mobile application on a smartphone, underwrite an insurance policy, or process an insurance claim or payment-card transaction, data related to individuals are the linchpin for servicing these orders. As a result, the GDPR's impact on U.S. FIs' handling of personal data was destined to have a widescale impact on operations. That impact tended to materialize in the following ways:

1. **Completing a data inventory.** In order to comply with Article 30 of the GDPR requiring a "record of processing" of all EU data, U.S. FIs embarked on extensive projects to record details about hundreds and thousands of applications, databases, devices, and vendors that often operated in clusters independent of each other. Because no single technology on the market could do all of this automatically, these initiatives necessarily involved hundreds and thousands of labor hours answering data-inventory surveys and completing in-person interviews. To better automate this capability, many U.S. FIs are exploring new technologies that rely to different degrees on "machine learning" to scan and classify their data assets.
2. **Operationalizing data-subject rights.** GDPR enhanced or created DSRs for EU residents to access, receive a copy of, correct, restrict processing of, or delete their data and to withdraw consent previously given to process their data. In the largest FIs, a single person's data could exist across dozens and even hundreds of systems often not synchronized with each other. Facing an uncertain volume of incoming DSRs after GDPR's effective date in May 2018—and lacking a single technology in the market to fully address this need—U.S. FIs developed predominantly manual processes to operationalize GDPR DSRs. To better automate this capability, many U.S. FIs are exploring updating or enhancing workflow-software solutions.
3. **Completing DPIAs.** GDPR introduced to U.S. FIs a requirement to document a data-protection impact assessment (DPIA) of new technology change involving EU personal data and to remediate risks to the "rights and freedoms" of individuals that are "high" as defined and understood by EU DPAs.¹ Remediating risks could involve reducing the data collected or how long it was retained, for example. For large FIs, this could mean conducting dozens or even hundreds of these assessments and related remediation projects each year. To better automate this capability, many U.S. FIs are exploring or enhancing workflow-software solutions.
4. **Updating third-party contracts.** The GDPR required "data controllers" to have contractual provisions holding their "data processors" accountable to the relevant provisions of the GDPR. The newer DSRs and data-breach notification threshold were among the more important provisions many opted to add explicitly to their contract addendums and service-level agreements. For U.S. FIs, the number of contracts needing updating could range from dozens to hundreds and even thousands. To better automate this capability, many U.S. FIs are exploring workflow-software solutions that rely to different degrees on machine learning.
5. **Appointing a DPO.** GDPR requires that organizations meeting certain conditions appoint a data protection officer (DPO), an "independent" person with direct access to leadership. For large FIs, addressing this could involve a single, full-time position or multiple positions that were internal staff or an outsourced firm. The GDPR offers further practical advantages for placing these DPOs in the FI's "main establishment" or main EU country of operations where they could more easily interact with their "lead" local data protection authority (DPA). In the run-up to the May 2018 deadline for GDPR, demand for DPOs grew rapidly and the available supply of qualified candidates diminished, complicating U.S. FIs' decisionmaking.
6. **Preparing to notify breaches within 72 hours.** The GDPR echoed a requirement from a New York State Department of Financial Services cybersecurity

¹See Article 29 Working Party WP247, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, October 2017, for examples of these "high-risk" criteria.

regulation whereby companies that experienced a compromise of EU personal data must notify relevant regulators within 72 hours of becoming aware of it. For FIs headquartered in the United States but operating in Europe, this meant expanding their U.S. breach-response capability into Europe—including associated staff, technologies, and supporting vendor relationships. A further challenge was informational—defining what could actually be known and reported within a relatively short window of time during which forensics investigations would often still be in progress.

- 7. Engaging the “first line of defense.”** One of the most important, ongoing challenges for U.S. FIs is to re-organize their data privacy organizations along the three “lines of defense” in order to give scalable and sustainable effect to GDPR controls. Many implemented a model based on placing privacy representatives in the business operations of the first line; data privacy governance leaders in the second line; and an oversight role in the third line. Traditionally, privacy expertise in the FI sector had been concentrated in the second line of defense. Identifying and equipping privacy representatives in the first line, whose primary jobs and training had not historically been data privacy, remains a general challenge for all commercial sectors.

Seven GDPR implementation insights for U.S. FIs

- 1. DSRs are not created equal.** The GDPR provides for eight data-subject rights: to privacy notices, to data access, to data rectification, to objection to processing, to withdrawal of consent for processing, to objection to automated processing, to data erasure, and to data portability. For most U.S. FIs, these were new requirements they were not previously subject to under U.S. data privacy regulations such as the GLBA Privacy Rule. The DSRs in the latter Rule were limited to a right to opt out of marketing and a right to opt out of data sharing with affiliates. The implementation and exercise of these new GDPR rights varied:
 - The GDPR rights generally posing the most implementation challenges for U.S. FIs were the rights to access and erasure. Fulfilling an access request could involve pulling information on an individual from dozens and even hundreds of structured databases and unstructured data stores—but doing so in a timely manner would probably require configuring all of these systems to a single consumer-identity-management system. Fulfilling an erasure request could in turn require different erasure and redaction protocols for each of these systems.
 - When consumers exercised their GDPR rights after May 2018, those most exercised generally were the rights to access, erasure, and objection to use for marketing.
- 2. Erased doesn’t mean forgotten.** The GDPR’s right to erasure is parenthetically referred to in the regulation as the “right to be forgotten,” although in practice in the U.S. financial industry, those two concepts may not be equivalent. The substantial number and scope of regulations and other obligations in the U.S. financial industry requiring the collection and retention of personal data such as for fraud prevention, cybersecurity, anti-money laundering, terrorist watchlisting, and for other discovery or litigation-related purposes means that U.S. FIs will limit or deny many requests for erasure. Moreover, for compliance purposes, U.S. FIs tend to keep a log of completed erasure requests that retains basic contact information of the requestor.
- 3. DSRs benefit from strong authentication.** For individuals, the GDPR right of access could produce files containing many personal details. If these files were delivered to the wrong individual, their privacy would be exposed. To counter this risk of misdirected files, companies can and do ask for multiple pieces of personal information from DSR requesters to first authenticate their identities before providing their requested files. A strong authentication process could also counter the risk of fraudulent DSR requests, which some U.S. FIs experienced in the year since GDPR went into effect. A challenge for this approach, however, is fulfilling DSRs for individuals for whom companies do not keep enough information to authenticate at a strong level. For example, a name and an email address may not be enough information to strongly authenticate.
- 4. The distinction between primary and secondary data controllers is important.** The GDPR does not distinguish between “primary” data controllers that maintain direct relationships with data subjects and “secondary” data controllers that do not. But this distinction is useful in the insurance industry, for

example, where direct insurers are positioned to provide privacy notices and data-breach notifications to data subjects and obtain consent and field DSRs from data subjects, whereby re-insurers are less well-positioned to do so.

5. **Board visibility makes a difference.** The prospect of being exposed to a fine of 4 percent of global revenues motivated many companies to implement their GDPR programs by May 2018, but the lack of any enforcement action approaching that monetary level in the year since GDPR took effect has reduced the pressure for ongoing enhancement of privacy controls in some quarters. U.S. FIs who routinized the reporting of their privacy program status to the Board or Audit Committee were more often successful in maintaining strong organizational support for GDPR during its first year of operation.
6. **Data governance is critical for privacy's success.** The GDPR emphasizes the need to have strong controls for personal data throughout its lifecycle of collection, storage, use, disclosure, and deletion. Because personal data often moves horizontally across vertically structured financial institutions, there is a heightened need in the financial industry to formalize an approach to data governance. For this reason, some FIs have endowed data governance leaders with some data privacy responsibilities.
7. **GDPR did not fully harmonize privacy regulation in Europe.** A benefit of the GDPR was to standardize many varying provisions in EU member states' data-protection laws, but substantial variations continue to exist. Accommodating regulatory variations generally increases the cost of compliance for FIs operating across multiple jurisdictions. To reduce their GDPR compliance and enforcement exposure, U.S. FIs are finding it necessary to continue to track variations at the EU member-state level where DPAs take the lead on enforcement and where class-action lawsuits are adjudicated. Member states, for example, are taking different approaches to the derogations left to them in the GDPR, different interpretations of "high risk" processing for DPIA purposes, and different enforcement priorities. The need to monitor these changes has tended to have a larger relative operational impact on smaller U.S. FIs operating in Europe because of their generally smaller data privacy teams.

Five unanswered questions for U.S. FIs post GDPR

As U.S. FIs continue to absorb the GDPR into their daily operations and plan for the future, they tend to share five common questions they are in the process of answering:

1. **Will the GDPR become the global data privacy standard?** As U.S. FIs operating internationally further automate their data privacy programs and capabilities, the cost of these enhancements is rising. Variances across jurisdictions regarding how these capabilities should be delivered to consumers—such as the specific nature and scope of DSRs—add to that cost. If GDPR DSRs will become the de facto global standard, it probably will make the most commercial sense for these multinationals to design their DSRs to be offered globally. If some GDPR DSRs won't become the global standard, however—such as the GDPR's right to opt out of automated decisionmaking—it would not make commercial sense to globalize those DSRs. Moreover, if GDPR's program accountability requirements become the global standard, it reduces the need and likelihood that the GLBA's right for customers to opt out of their nonpublic personal data being shared with affiliates of the FI will become a standard outside the United States. U.S. FIs engaging in long-term, strategic planning for their data usage are needing to answer this question.
2. **Will people increasingly exercise their privacy rights?** Many U.S. companies received under 100 GDPR DSRs in the year after GDPR went into effect, while some outliers fielded thousands of them. In some cases, U.S. residents attempted to exercise GDPR rights. Companies receiving them had to decide whether to reject them on legal grounds or fulfill them in order to provide a positive consumer experience. Most U.S. healthcare providers and insurers similarly receive fewer than 100 HIPAA DSRs each year. As the California Consumer Privacy Act (CCPA) brings to many U.S. companies for the first time the rights to access and erasure and to opt out of selling data to third parties, questions many U.S. privacy leaders are asking is whether their expected volume of DSRs will outstrip their generally manual processes for fulfilling DSRs, and whether residents outside California will attempt to exercise these rights in large numbers.
3. **How can informed consent be facilitated in a blink?** The sharp rise in the use of pop-up windows on mobile and stationary websites to capture user

consent for cookies has slowed down the typical online customer experience to demonstrate compliance without offering an obvious material improvement in privacy protection. Corporate privacy leaders are looking for new models—such as mobile apps that ask you if you want to enable that app tracking your device’s geolocation or accessing your contacts—that break down the privacy-consent process into quicker, more meaningful steps.

4. **What pseudonymization protocol will stand the test of time?** Effective pseudonymization can increase the ability to use and monetize data and create commercial innovation while also protecting individual privacy. Advances in data processing and artificial intelligence, however, are changing the threshold of what is identifiable data and how much has to be removed from a data set in order for it to be pseudonymized, anonymized, or de-identified. U.S. privacy leaders are looking toward the “statistical” method of de-identification described in the Health Insurance Portability and Accountability Act (HIPAA) as a potential answer to this question.
5. **What is a high risk to privacy?** Effectively functioning companies will allocate the most risk-management resources to address risks they determine are “high” in their enterprise risk-management (ERM) programs. The concept of high risk embedded in the GDPR and interpreted in varying ways across EU member states diverges in many ways from the concept of high risk provided for in different U.S. data privacy laws. For example, the GDPR considers a person’s status with regard to membership in a trade union as “sensitive” data whose processing creates inherent high risk, while no U.S. privacy law or regulation results in a similar determination. Conversely, U.S. data-breach notification laws make the storage of Social Security numbers an inherent high risk, but GDPR does not similarly classify the processing of EU social-insurance numbers. Similarly, EU DPAs have listed “large-scale data processing” as a high-risk criterion that does not have an equivalent in U.S. privacy regulations. Unless these concepts converge over time across jurisdictions, privacy risk management may need to be regionalized in several respects.

Looking ahead

The GDPR has caused U.S. FIs to implement new ways for European residents to control their personal data. The GDPR’s extraterritorial reach has in turn prompted other jurisdictions around the world to adopt its model that is centered on offering a set of data-subject rights and instituting programmatic controls. To plan for a future where consumers around the world may generally expect the core rights of access, deletion, and objection to marketing, many U.S. FIs are redesigning their privacy organizational models and capabilities. Because of the relative newness of technologies designed to automate the fulfillment of privacy rights and the technical complexity of many FIs, a significant effort lies ahead of them in realizing these designs. A key factor in whether automation is needed or manual processes will continue to suffice is the degree to which consumers will increasingly demand these rights. As these factors converge, the highest level of privacy protection in the digital age will result when both companies and consumers exercise their roles to the fullest.

PREPARED STATEMENT OF MACIEJ CEGLOWSKI

FOUNDER, PINBOARD

MAY 7, 2019

Thank you for the opportunity to address you today.

I am the founder and sole employee of Pinboard, a small for-profit archiving service founded in 2009 that competes in part on the basis of personal privacy. I have also been a frequent critic of Silicon Valley’s reliance on business models requiring mass surveillance, speaking on the topic at conferences both in the United States and abroad.

As someone who earns his living through data collection, I am acutely aware of the power the tools we are building give us over our fellow citizens’ private lives, and the danger they pose to our liberty. I am grateful to Chairman Crapo, ranking Member Brown, and the Committee for the opportunity to testify on this vital matter.

The internet economy in 2019 is dominated by five American tech companies: Apple, Microsoft, Google, Facebook, and Amazon. These are also the five most valuable corporations in the world, with a combined market capitalization exceeding four

trillion dollars.¹ Between them, these companies control the market for online advertising, mobile and desktop operating systems, office software, document storage, search, cloud computing, and many other areas of the digital economy. They also own and operate a significant portion of the physical infrastructure of the internet, and act as its *de facto* regulating authority.

The concentration of power in the hands of these giant firms is the epilogue to a spectacular story of American innovation and dynamism. The technologies underpinning the internet were all developed here in the United States, and the many fortunes that they produced owe their thanks to fruitful cooperation between Government, industry, and the research community. Working together, the public and private sectors created the conditions for a startup culture unlike any other in the world.

Today, however, that culture of dynamism is at risk. The surveillance business model has eroded user trust to such a point that it is impeding our ability to innovate.

In many ways, the five internet giants operate like sovereign states. Their operations are global, and decisions they take unilaterally can affect entire societies. Denmark has gone so far as to send an ambassador to Silicon Valley. When Jeff Bezos, the CEO of Amazon, met recently with the Canadian prime minister, the occasion was covered in the press like a state visit.

The emergence of this tech oligopoly reflects a profound shift in our society, the migration of every area of commercial, social, and personal life into an online realm where human interactions are mediated by software.

To an extent that has no precedent, the daily activities of most Americans are now tracked and permanently recorded by automated systems. It is likely that every person in this hearing room carries with them a mobile phone that keeps a history of their location, is privy to their most private conversations, and contains a rich history of their private life. Some of you may even have an always-on microphone in your car or home that responds to your voice commands.

Emerging technologies promise to afford these systems even more intimate glimpses into our private lives—phones that monitor our facial expressions as we read, and connected homes that watch over us while we sleep. Scenarios that were once the province of dystopian dime fiction have become an unremarkable consumer reality.

The sudden ubiquity of this architecture of mass surveillance, and its enshrinement as the default business model of the online economy, mean that we can no longer put off hard conversations about the threats it poses to liberty.

Adding to this urgency is the empirical fact that, while our online economy depends on the collection and permanent storage of highly personal data, we do not have the capacity to keep such large collections of user data safe over time.

The litany of known data breaches is too long to recite here, but includes every one of the top five tech companies, as well as health and financial firms and Government agencies. Every year brings new and more spectacular examples of our inability to protect our users. At Yahoo, an internet giant at the time with a world-class security team, over 3 billion user accounts were compromised in a 2013 breach. In 2015, the U.S. Office of Personnel Management allowed unauthorized access to the records of over four million people, including many with highly sensitive security clearances. And in 2017, Equifax exposed data, including Social Security numbers, on 147 million Americans, nearly half the U.S. population.

While many individual data breaches are due to negligence or poor practices, their overall number reflects an uncomfortable truth well known to computer professionals—that our ability to attack computer systems far exceeds our ability to defend them, and will for the foreseeable future.

The current situation, therefore, is not tenable. The internet economy today resembles the earliest days of the nuclear industry. We have a technology of unprecedented potential, we have made glowing promises about how it will transform the daily lives of our fellow Americans, but we don't know how to keep its dangerous byproducts safe.

Two Views of Privacy

Discussing privacy in the context of regulation can be vexing, because the companies doing the most to erode our privacy are equally sincere in their conviction that they are its champions.

The confusion stems from two different ways in which we use the word privacy, leading us to sometimes talk past each other.

¹At the time of writing, Amazon was valued at \$966B, Microsoft \$988B, Apple \$974B, Facebook \$558B, and Google (Alphabet) \$824B.

In the regulatory context, discussion of privacy invariably means data privacy—the idea of protecting designated sensitive material from unauthorized access.

Laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) delimit certain categories of sensitive information that require extra protection, and mandate ways in which health and financial institutions have to safeguard this data, or report when those safeguards have failed. The Children’s Online Privacy Protection Act of 1998 extends similar protection to all data associated with children.

We continue to use this framework of data privacy today, including in the recently enacted General Data Protection Regulation (GDPR).

It is true that, when it comes to protecting specific collections of data, the companies that profit most from the surveillance economy are the ones working hardest to defend them against unauthorized access.

But there is a second, more fundamental sense of the word privacy, one which until recently was so common and unremarkable that it would have made no sense to try to describe it.

That is the idea that there exists a sphere of life that should remain outside public scrutiny, in which we can be sure that our words, actions, thoughts and feelings are not being indelibly recorded. This includes not only intimate spaces like the home, but also the many semi-private places where people gather and engage with one another in the common activities of daily life—the workplace, church, club or union hall. As these interactions move online, our privacy in this deeper sense withers away.

Until recently, even people living in a police state could count on the fact that the authorities didn’t have enough equipment or manpower to observe everyone, everywhere,² and so enjoyed more freedom from monitoring than we do living in a free society today.

A characteristic of this new world of ambient surveillance is that we cannot opt out of it, any more than we might opt out of automobile culture by refusing to drive. However sincere our commitment to walking, the world around us would still be a world built for cars. We would still have to contend with roads, traffic jams, air pollution, and run the risk of being hit by a bus.

Similarly, while it is possible in principle to throw one’s laptop into the sea and renounce all technology, it is no longer possible to opt out of a surveillance society.

When we talk about privacy in this second, more basic sense, the giant tech companies are not the guardians of privacy, but its gravediggers.

The tension between these interpretations of what privacy entails, and who is trying to defend it, complicates attempts to discuss regulation.

Tech companies will correctly point out that their customers have willingly traded their private data for an almost miraculous collection of useful services, services that have unquestionably made their lives better, and that the business model that allows them to offer these services for free creates far more value than harm for their customers.

Consumers will just as rightly point out that they never consented to be the subjects in an uncontrolled social experiment, that the companies engaged in reshaping our world have consistently refused to honestly discuss their business models or data collection practices, and that in a democratic society, profound social change requires consensus and accountability.

Behavioral Data

Further complicating the debate on privacy is the novel nature of the data being collected. While the laws around protecting data have always focused on intentional communications—documents that can be intercepted, conversations that can be eavesdropped upon—much of what computer systems capture about us is behavioral data: incidental observations of human behavior that don’t seem to convey any information at all.

Behavioral data encompasses anything people do while interacting with a computer system. It can include the queries we type into a search engine, our physical location, the hyperlinks we click on, whether we are sitting or standing, how quickly we scroll down a document, how jauntily we walk down a corridor, whether our eyes linger on a photo, whether we start to write a comment and then delete it—even the changes in our facial expression as we are shown an online ad.

²The record for intensive surveillance in the pre-internet age likely belongs to East Germany, where by some estimates one in seven people was an informant; <https://archive.nytimes.com/www.nytimes.com/books/first/k/koebler-stasi.html>.

This incidental data has proven to be such a valuable raw material that an entire industry now specializes in finding ways to mine it. The devices used to spy on us include our computers, cell phones, televisions, cars, security cameras, our children's toys, home appliances, wifi access points, even at one point trash cans in the street.³

Privacy and Consent

The extent to which anyone consents—or *can* consent—to this kind of tracking is the thorny question in attempting to regulate the relationship between people and software.

The General Data Protection Regulation (GDPR), enacted in May 2018, is the most ambitious attempt thus far to regulate online privacy. It takes a very traditional view of the relationship between people and data.

In the eyes of the GDPR, people own their data. They make an affirmative choice to share their data with online services, and can revoke that choice. The consent they give must be explicit and limited to a specified purpose—the recipient does not have *carte blanche* to use the data as they please, or to share it with third parties, with some complicating caveats.

People have the right to request a full download of their data from the services they have entrusted it to, and they have the right to demand that it be permanently erased.

The GDPR imposes a notification requirement for data breaches, and requires affirmative consent for the sale of user data. It also restricts the movement of data to outside jurisdictions (though in the case of the United States, this restriction is superseded by the U.S.-EU Privacy Shield framework).

Finally, the GDPR mandates that privacy safeguards like data tokenization and encryption be built in to new systems, and that companies appoint a dedicated privacy officer.

The GDPR is not a simple regulation, and many of its most potentially significant provisions (such as the scope of a data controller's "legitimate interests," or what the right to erasure means in the context of a machine learning model) await interpretation by regulators.

What limits, if any, the GDPR will place on the application of machine learning is a particularly important open question. The law on its face prohibits automated decisionmaking that has a "legal or similarly significant effect" on data subjects, but the definition of "significant effect" is not clear, nor is it clear whether having a human being simply countersign an algorithmic decision would be enough to satisfy regulators that the decision process is not fully automated.

Impacts

As it is so new, the GDPR's ultimate impact on online privacy in the European Union is unclear. Some of the dramatic early impacts (like major U.S. newspapers going offline) have proven to be transient, while many of the biggest impacts hinge on future decisions by EU regulators.

Enough has happened, however, to draw some preliminary conclusions.

The GDPR so far has made life hard on internet users. It is not clear that this is the GDPR's fault.

The plain language of the GDPR is so plainly at odds with the business model of surveillance advertising that contorting the real-time ad brokerages into something resembling compliance has required acrobatics that have left essentially everybody unhappy.

The leading ad networks in the European Union have chosen to respond to the GDPR by stitching together a sort of Frankenstein's monster of consent, a mechanism whereby a user wishing to visit, say, a weather forecast page⁴ is first prompted to agree to share data with a consortium of 119 entities, including the aptly named "A Million Ads" network. The user can scroll through this list of intermediaries one by one, or give or withhold consent *en bloc*, but either way she must wait a further 2 minutes for the consent collection process to terminate before she is allowed to find out whether or not it is going to rain.

This majestically baroque consent mechanism also hinders Europeans from using the privacy preserving features built into their web browsers, or from turning off invasive tracking technologies like third-party cookies, since the mechanism depends on their being present.

³ Campbell-Dollaghan, Kelsey. "Brave New Garbage: London's Trash Cans Track You Using Your Smartphone." Gizmodo. (Aug. 9, 2013), <https://gizmodo.com/brave-new-garbage-londons-trash-cans-track-you-using-1071610114>.

⁴ This is an actual example.

For the average EU citizen, therefore, the immediate effect of the GDPR has been to add friction to their internet browsing experience along the lines of the infamous 2011 EU Privacy Directive (“EU cookie law”) that added consent dialogs to nearly every site on the internet.

The GDPR rollout has also demonstrated to what extent the European ad market depends on Google, who has assumed the role of *de facto* technical regulatory authority due to its overwhelming market share.⁵ Google waited until the night before the regulation went into effect to announce its intentions, leaving ad networks scrambling.

It is significant that Google and Facebook also took advantage of the U.S.-EU privacy shield to move 1.5 billion non-EU user records out of EU jurisdiction to servers in the United States. Overall, the GDPR has significantly strengthened Facebook and Google at the expense of smaller players in the surveillance economy.

The data protection provisions of the GDPR, particularly the right to erase, imposed significant compliance costs on internet companies. In some cases, these compliance costs just show the legislation working as intended. Companies who were not keeping adequate track of personal data were forced to retrofit costly controls, and that data is now safer for it.

But in other cases, companies with a strong commitment to privacy also found themselves expending significant resources on retooling. Personally identifying information has a way of seeping in to odd corners of computer systems (for example, users will sometimes accidentally paste their password into a search box), and tracking down all of these special cases can be challenging in a complex system. The requirements around erasure, particularly as they interact with backups, also impose a special burden, as most computer systems are designed with a bias to never losing data, rather than making it easy to expunge.

A final, and extremely interesting outcome of the GDPR, was an inadvertent experiment conducted by the New York Times. Privacy advocates have long argued that intrusive third-party advertising does not provide more value to publishers than the traditional pre-internet style of advertising based off of content, but there has never been a major publisher willing to publicly run the experiment.

The New York Times tested this theory by cutting off all ad networks in Europe, and running only direct sold ads to its European visitors. The paper found that ad revenue increased significantly, and stayed elevated into 2019, bolstering the argument that surveillance-based advertising offers no advantage to publishers, and may in fact harm them.⁶

The Limits of Consent

While it is too soon to draw definitive conclusions about the GDPR, there is a tension between its concept of user consent and the reality of a surveillance economy that is worth examining in more detail.

A key assumption of the consent model is any user can choose to withhold consent from online services. But not all services are created equal—there are some that you really can’t say no to.

Take the example of Facebook. Both landlords and employers in the United States have begun demanding to see Facebook accounts as a condition of housing or employment.⁷ The United States Border Patrol has made a formal request to begin collecting social media to help vet people arriving in the country.⁸ In both those contexts, not having a Facebook account might stand out too much to be a viable option. Many schools now communicate with parents via Facebook; Facebook groups are also the locus for political organizing and online activism across the political spectrum.

Analogous arguments can be made for social products offered by the other major tech companies. But if you can’t afford to opt out, what does it mean to consent?

⁵Google has at least a 70 percent advertising market share in Europe, though this figure is averaged over the 10 year period 2006–2016 and likely far higher today. Laurent, Lionel. “Europe Is Changing Google for the Better.” Washington Post. (March 20, 2019), https://www.washingtonpost.com/business/europe-is-changing-google-for-the-better/2019/03/20/691aaff4-4b2e-11e9-8cfc-2c5d0999c21e_story.html.

⁶Davies, Jessica. “After GDPR, the New York Times cutoff ad exchanges in Europe—and kept growing ad revenue.” Digiday. Jan. 6, 2019, <https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/>.

⁷Dewey, Caitlin. “Creepy startup will help landlords, employers and online dates strip-mine intimate data from your Facebook page.” Washington Post. June 9, 2016, <https://www.washingtonpost.com/news/the-intersect/wp/2016/06/09/creepy-startup-will-help-landlords-employers-and-online-dates-strip-mine-intimate-data-from-your-facebook-page/>.

⁸81 FR 40892. <https://www.federalregister.gov/documents/2016/06/23/2016-14848/agency-information-collection-activities-arrival-and-departure-record-forms-i-94-and-i-94w-and-h-11>.

Opting out can also be impossible because of how deeply the internet giants have embedded themselves in the fabric of the internet. For example, major media properties in the European Union use a technology called ReCaptcha on their GDPR consent forms.⁹ These forms must be completed before a user can access the website they are gathering consent for, but since the ReCaptcha service is run by Google, and the form cannot be submitted without completing the Google-generated challenge (which incidentally performs free image classification labor for the company), a user who refuses to give Google access to her browser will find herself denied access to a large portion of the internet.

While this specific example may change when it comes to the attention of an EU regulator, the broader issue remains. The sheer reach of the tech oligopoly makes it impossible to avoid using their services. When a company like Google controls the market-leading browser, mobile operating system, email service and analytics suite, exercises a monopoly over search in the European Union, runs the largest ad network in Europe, and happens to own many of the undersea cables that connect Europe to the rest of the world,¹⁰ how do you possibly say “no”?

Informed Consent

Beyond one’s basic ability to consent, there is the question of what it means to give informed consent. Presumably we are not opting in or out of the services we use for capricious reasons, but because we can make a rational choice about what is in our interest.

In practice, however, obtaining this information is not possible, even assuming superhuman reserves of patience.

For example, anyone visiting the popular Tumblr blogging platform from a European IP address must first decide whether to share data with Tumblr’s 201 advertising partners, and read five separate privacy policies from Tumblr’s several web analytics providers.

Despite being a domain expert in the field, and spending an hour clicking into these policies, I am unable to communicate what it is that Tumblr is tracking, or what data of mine will be used for what purposes by their data partners (each of whom has its own voluminous terms of service). This opacity exists in part because the intermediaries have fought hard to keep their business practices and data sharing processes a secret, even in the teeth of strong European regulation.

Organizations like the Interactive Advertising Bureau Europe (IABE) defeat the spirit of the GDPR by bundling consent and requiring it across many ad-supported properties in Europe. If regulators block the bundling in its current incarnation, it will no doubt rise from the dead in a modified form, reflecting the undying spirit of surveillance advertising. But at no point will internet users have the information they would need to make a truly informed choice (leaving aside the ridiculousness of requiring a legal education and 2 hours of sustained close reading in order to watch a cat video).

Consent in a world of inference

Finally, there is a sense in which machine learning and the power of predictive inference may be making the whole idea of consent irrelevant. At this point, companies have collected so much data about entire populations that they can simply make guesses about us, often with astonishing accuracy.¹¹

A useful analogy here is a jigsaw puzzle. If you give me a puzzle with one piece missing, I can still assemble it, reconstruct the contours of the missing piece by looking at the shape of the pieces around it and, if the piece is small compared to the whole, easily interpolate the missing part of the image.

This is exactly what computer systems do to us when we deny them our personal information. Experts have long known that it takes a very small amount of data to make reliable inferences about a person. Most people in the United States, for

⁹The purpose of ReCaptcha is to prevent automated submissions, and ensure that a human being is filling out the form.

¹⁰Zimmer, Jameson. “Google Owns 63,605 Miles and 8.5 percent of Submarine Cables Worldwide.” *Broadband Now*. (September 12, 2018), <https://broadbandnow.com/report/google-content-providers-submarine-cable-ownership/>.

¹¹The line of argument in this section is adapted from the work of Dr. Zeynep Tufekci, UNC Chapel Hill. For example, “Think You’re Discreet Online? Think Again,” (April 21, 2019), <https://www.nytimes.com/2019/04/21/opinion/computational-inference.html>.

example, can be uniquely identified by just the combination of their date of birth, gender, and ZIP Code.¹²

But machine learning is honing this ability to fill in the blanks to surprising levels of accuracy, raising troubling questions about what it means to have any categories of protected data at all.

For example, imagine that an algorithm could inspect your online purchasing history and, with high confidence, infer that you suffer from an anxiety disorder. Ordinarily, this kind of sensitive medical information would be protected by HIPAA, but is the inference similarly protected? What if the algorithm is only reasonably certain? What if the algorithm knows that you're healthy now, but will suffer from such a disorder in the future?

The question is not hypothetical—a 2017 study¹³ showed that a machine learning algorithm examining photos posted to the image-sharing site Instagram was able to detect signs of depression before it was diagnosed in the subjects, and outperformed medical doctors on the task.

The paradigm of automatic ownership of personal data does not mesh well with a world where such private data cannot only interpolated and reconstructed, but independently discovered by an algorithm!

And if I can infer such important facts about your life by applying machine learning to public data, then I have deprived you of privacy just as effectively as I would have by direct eavesdropping.

In order to talk meaningfully about consent in online systems, the locus of regulation will need to expand beyond data collection, to cover how those data collections, and the algorithms trained on them, are used. But to do this, we will first need far greater visibility into the workings of surveillance-dependent tech companies than they have so far been willing to grant us.

As it stands, the consent framework exemplified in the GDPR is simply not adequate to safeguard privacy. As much as we would like to be the masters of our data, we are not. And the real masters aren't talking.

Goals for Privacy Regulation

Absent a clear understanding of how our data is being used, and the role it plays in surveillance-based business models, it is hard to lay out a specific regulatory program.

Nevertheless, there are some general goals we can pursue based on the experience of regulation attempts in Europe, and what we know about the surveillance economy.

Clarity

Privacy regulation should be understandable, both for users of the technology, and for the companies the regulations govern. Users especially should not be required to make complex and irrevocable decisions about privacy. To the extent possible, intuitions about privacy from the human world ("a casual conversation between friends is not recorded forever") should carry over into the digital world.

Privacy

At the risk of sounding tautological, privacy regulation should not punish people for seeking privacy. It should not be necessary to turn on invasive tracking technologies in one's browser in order to express the desire to not to be tracked.

Retention Limits on Behavioral Data

Knowing that we lack the capacity to keep data collections safe over time, we can reduce the potential impact of any breach by setting strict lifetimes for behavioral data.

Google has demonstrated the feasibility of this approach with their recent announcement that users will be able to set their account to automatically delete location data after 3 or 18 months.¹⁴ This demonstrates that permanent retention of behavioral data is not critical to surveillance-based business models. Such limits should be enforced industrywide.

¹²Sweeney, Latanya. "Simple Demographics Often Identify People Uniquely," Carnegie Mellon University, Data Privacy Working Paper. (2000), <https://dataprivacylab.org/projects/identifiability/paper1.pdf>.

¹³Reece, Andrew and Danforth, Christopher. "Instagram photos reveal predictive markers of depression." *EPJ Data Science*, (2017), <https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-017-0110-z>.

¹⁴Monsees, David and McGriff, Marlo. "Introducing auto-delete controls for your Location History and activity data." (May 1, 2019), <https://www.blog.google/technology/safety-security/automatically-delete-data/>.

Moving to a norm where behavioral data is kept briefly instead of forever will mark a major step forward in data security, both reducing the time data is potentially exposed to attackers, and reducing the total volume of data that must be kept safe.

Time limits on behavioral data will also reduce consumers' perception that they are making irrevocable privacy commitments every time they try a new product or service.

Right To Download

The right to download is one of the most laudable features in the GDPR, and serves the important secondary purpose of educating the public about the extent of data collection.

This right should, however, be expanded to include the right to download, and correct, all information that third-party data brokers have provided about a user, in a spirit similar to the Fair Credit Reporting Act.

Fairness

Tech startups in the highly regulated areas of health, finance and banking should be required to compete on the same regulatory footing as established businesses in those areas. In particular, they should not be allowed to do an end run around existing data privacy laws by using machine learning and algorithmic inference.

For example, the use of a machine learning algorithm should not allow a loan company to evade consumer protections against discrimination in fair lending laws. (For a fuller discussion of this point, see the addendum on machine learning at the end of this document).

Positive Regulation

While the above suggestions seek to impose limits and restrictions, there is an important way that privacy regulation can create new ground for innovation.

What is missing from the regulatory landscape is a legal mechanism for making credible and binding promises to users about privacy practices.

Today, internet startups in the United States who want to compete on privacy have no mechanism to signal their commitment to users other than making promises through their terms of service (which usually include a standard legal clause that they may change at any time).

Except in the case of the most egregious violations, which sometimes attract the attention of the Federal Trade Commission, these terms of service carry little weight.

As the owner of a company that markets itself to privacy-conscious people, I would derive enormous benefit from a legal framework that allowed me to make binding privacy promises (for example, a pledge that there is no third-party tracking on my website), and imposed stiff fines on my company if I violated these guarantees (including criminal liability in the case of outright fraud).

Such a legal mechanism would not only enable competition around privacy-enhancing features, but it would also give future regulators a clearer idea of how much value consumers place on data privacy. It is possible that the tech giants are right, and people want services for free, no matter the privacy cost. It is also possible that people value privacy, and will pay extra for it, just like many people now pay a premium for organic fruit. The experiment is easy to run—but it requires a modest foundation in law.

Academic research in computer science is full of fascinating ideas that could serve as the seed for business built around user privacy. Results in fields like homomorphic encryption, differential privacy, privacy-preserving machine learning, and zero-knowledge proofs all await a clever entrepreneur who can incorporate them into a useful product or service. It is very hard to compete against companies like Amazon or Facebook on price, but it is not hard to beat them on privacy. With a minimum of regulatory scaffolding, we might see a welcome new burst of innovation.

Preserving Liberty

The final, and paramount goal, of privacy regulation should be to preserve our liberty.

There is no clearer warning of the danger of building up an infrastructure of surveillance than what is happening today in China's Xinjiang Uygur Autonomous Region. Claiming to be concerned about the possible radicalization of a Muslim minority, Chinese authorities have imposed a regime of total surveillance over a population of 25 million people.

As recent reporting by Human Rights Watch has shown, a computer system called the Integrated Joint Operations Platform (IJOP) monitors the location and move-

ment of all people in the province (based on phone data), as well as their gas and electricity consumption, which apps they use, where they worship, who they communicate with, and how they spend their money. This surveillance information is fed into machine learning models that can bin people into one of 36 suspect categories, bringing them to the closer attention of the police.¹⁵ Never before has a government had the technical means to implement this level of surveillance across an entire population. And they are doing it with the same off-the-shelf commercial technologies we use in America to get people to click on ads.

The latent potential of the surveillance economy as a toolkit for despotism cannot be exaggerated. The monitoring tools we see in repressive regimes are not “dual use” technologies—they are single use technologies, working as designed, except for a different master.

For 60 years, we have called the threat of totalitarian surveillance “Orwellian,” but the word no longer fits the threat. The better word now may be “Californian.” A truly sophisticated system of social control, of the kind being pioneered in China, will not compel obedience, but nudge people toward it. Rather than censoring or punishing those who dissent, it will simply make sure their voices are not heard. It will reward complacent behavior, and sideline troublemakers. It’s even possible that, judiciously wielded, such a system of social control might enjoy wide public support in our own country.

But I hope you will agree with me that such a future would be profoundly un-American.

There is no deep reason that weds the commercial internet to a business model of blanket surveillance. The spirit of innovation is not dead in Silicon Valley, and there are other ways we can grow our digital economy that will maintain our lead in information technology, while also safeguarding our liberty. Just like the creation of the internet itself, the effort to put it on a safer foundation will require a combination of research, entrepreneurial drive and timely, enlightened regulation. But we did it before, and there’s no reason to think we can’t do it again.

Addendum: Machine Learning and Privacy

Machine learning is a mathematical technique for training computer systems to make accurate predictions from a large corpus of training data, with a degree of accuracy that in some domains can mimic human cognition.

For example, machine learning algorithms trained on a sufficiently large data set can learn to identify objects in photographs with a high degree of accuracy, transcribe spoken language to text, translate texts between languages, or flag anomalous behavior on a surveillance videotape.

The mathematical techniques underpinning machine learning, like convolutional neural networks (CNN), have been well-known since before the revolution in machine learning that took place beginning in 2012. What enabled the key breakthrough in machine learning was the arrival of truly large collections of data, along with concomitant computing power, allowing these techniques to finally demonstrate their full potential.

It takes data sets of millions or billions of items, along with considerable computing power, to get adequate results from a machine learning algorithms. Before the advent of the surveillance economy, we simply did not realize the power of these techniques when applied at scale.

Because machine learning has a voracious appetite for data and computing power, it contributes both to the centralizing tendency that has consolidated the tech industry, and to the pressure companies face to maximize the collection of user data.

Machine learning models poses some unique problems in privacy regulation because of the way they can obscure the links between the data used to train them and their ultimate behavior.

A key feature of machine learning is that it occurs in separable phases. An initial training phase consists of running a learning algorithm on a large collection of labeled data (a time and computation-intensive process). This model can then be deployed in an exploitation phase, which requires far fewer resources.

Once the training phase is complete, the data used to train the model is no longer required and can conceivably be thrown away.

The two phases of training and exploitation can occur far away from each other both in space and time. The legal status of models trained on personal data under privacy laws like the GDPR, or whether data transfer laws apply to moving a trained model across jurisdictions, is not clear.

¹⁵Human Rights Watch, “China’s Algorithms of Repression,” (May 1, 2019), <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance>.

Inspecting a trained model reveals nothing about the data that went into it. To a human inspecting it, the model consists of millions and millions of numeric weights that have no obvious meaning, or relationship to human categories of thought. One cannot examine an image recognition model, for example, and point to the numbers that encode “apple.”

The training process behaves as a kind of one-way function. It is not possible to run a trained model backwards to reconstruct the input data; nor is it possible to “untrain” a model so that it will forget a specific part of its input.

Machine learning algorithms are best understood as inference engines. They find structure and excel at making inferences from data that can sometimes be surprising even to people familiar with the technology. This ability to see patterns that humans don’t notice has led to interest in using machine learning algorithms in medical diagnosis, evaluating insurance risk, assigning credit scores, stock trading, and other fields that currently rely on expert human analysis.

The opacity of machine learning models, combined with this capacity for inference, also make them an ideal technology for circumventing legal protections on data use. In this spirit, I have previously referred to machine learning as “money laundering for bias.” Whatever latent biases are in the training data, whether or not they are apparent to humans, and whether or not attempts are made to remove them from the data set, will be reflected in the behavior of the model.

A final feature of machine learning is that it is curiously vulnerable to adversarial inputs. For example, an image classifier that correctly identifies a picture of a horse might reclassify the same image as an apple, sailboat or any other object of an attacker’s choosing if they can manipulate even one pixel in the image.¹⁶ Changes in input data not noticeable to a human observer will be sufficient to persuade the model. Recent research suggests that this property is an inherent and ineradicable feature of any machine learning system that uses current approaches.¹⁷

In brief, machine learning is effective, has an enormous appetite for data, requires large computational resources, makes decisions that resist analysis, excels at finding latent structure in data, obscures the link between source data and outcomes, defies many human intuitions, and is readily fooled by a knowledgeable adversary.

¹⁶Su, Jiawei, Vargas, Danilo, and Kouichi, Sakurai. “One Pixel Attack for Fooling Deep Neural Networks.” (Oct 24, 2017), <https://arxiv.org/pdf/1710.08864.pdf>.

¹⁷Wang, Xianmin, Li, Jing, Kuang, Xiaohui, Tan, Yu-an. “The security of machine learning in an adversarial setting: A survey.” *Journal of Parallel and Distributed Computing*, (August 2019).

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR
MENENDEZ FROM PETER H. CHASE**

Q.1. We are approaching the 1-year anniversary of the GDPR. What are some of the negative unintended consequences that the United States can learn from as Congress explores its own privacy legislation?

A.1. There have been a number of stories about some of the negative unintended consequences of GDPR in its first year in force. One study (<https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment>) found that venture capital for tech firms in Europe declined significantly compared with counterparts in the United States, noting specifically:

EU technology firms, on average, experienced double-digit percentage declines in venture funding relative to their U.S. counterparts after GDPR went into effect. At our aggregate unit of observation, EU venture funding decreased by \$3.38 million at the mean of \$23.18 million raised per week per state per crude technology category. This reduction takes place in both the intensive margin (the average dollar amount raised per round of funding, which decreased 39 percent) and the extensive margin (the number of deals, which incurred a 17 percent average drop).

GDPR's effect is particularly pronounced for young (0–3 year-old) EU ventures, where an average reduction of 19 percent in the number of deals is observed . . . If GDPR leads to fewer new ventures and less capital per venture, there could be fewer jobs as a result. Our back-of-the-envelope calculation suggests that the investment reduction for young ventures could translate into a yearly loss between 3,604 to 29,819 jobs in the European Union, corresponding to 4.09 percent to 11.20 percent of jobs created by 0–3 year-old ventures in our sample.¹

The authors of the study note that this effect may not be due to the GDPR *per se*, but rather to the actions major platforms took to ensure that apps available through them were GDPR-compliant. They also stress that this is a short-run observation, which could correct over time.

Somewhat related, I have been told by representatives of major financial firms involved in mergers and acquisitions that the need for “due diligence” related to GDPR compliance has become a significant factor in slowing some deals.

¹Jian Jia *et al.*, *The Short-Run Effects of GDPR on Technology Venture Investment*, *Vox.eu*, (January 7, 2019).

Another consequence, which probably is unintended in its magnitude and direction, appears to have been on hospitals that have increasingly moved toward digitalization of their healthcare-related services, as these have had to invest considerably more in compliance than less technologically advanced hospitals, including with respect to staff training.²

Unintended negative consequences such as these must be expected with any large and detailed law, and especially one that affects the practices of virtually all businesses, as all firms—not just the IT sector—have become digital. As noted in my written statement, certainly an expected consequence was the cost of compliance, although European authorities may have under-estimated those costs. One possible reason for this is that even in its own publications, the European Union and many others have stressed the somewhat absolutist aspect of the “fundamental right” to data protection, although in fact GDPR does take more of a risk-based approach. This has been beneficial for the many large and small firms that have leapt into the GDPR compliance business.

But these unintended costs are also offset by some unexpected benefits, such as those that appear to have come from extended “data hygiene” processes many firms have undergone, including with respect to their cyber-security practices.³

Q.2. A central element of GDPR is that companies must clearly explain how data is collected and used. Already we’ve seen companies such as Google face heavy fines for failing to comply with GDPR’s consent requirements. How would you grade the EU’s enforcement of GDPR standards writ large, but also specifically the data collection and use standards?

A.2. GDPR has notably raised awareness of the importance of data protection in the European Union, among citizens as well as firms that hold consumer data. This is important, as the first step in GDPR enforcement comes from citizens exercising their rights to more information about what data is being collected about them and how it is being used. GDPR gives them a right to lodge complaints with a data protection authority, and to seek effective judicial remedies both against that authority (e.g., for not acting on a complaint) and a data controller or processor. GDPR also allows not-for-profit civil society organizations versed in data protection issues to lodge such complaints, as Privacy International recently did against a number of data brokers and credit rating agencies.

Actual enforcement rests in the first instance on the Data Protection Supervisory Authorities in each of the EU member states, which may take differing approaches to this task. Some are more focused on helping firms—especially smaller ones—comply with their obligations under GDPR; others may be more disciplinary. That being said, the European Data Protection Board (EDPB) provides guidance and rulings to ensure the member state DPSAs interpret the GDPR in a consistent manner.

²Yuan Bocong and Li Jiannan, *The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation*, International Journal of Environmental Research and Public Health, March 25, 2019. (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6466053/>)

³Tim Woods, *GDPR’s Impact on Incident Response*, Security Today, April 24, 2019. <https://securitytoday.com/Articles/2019/04/24/GDPRs-Impact-on-Incident-Response.aspx?Page=1>.

On May 22, 2019, the EDPB published a blog “taking stock” of the GDPR, noting that member state supervisory authorities received 144,376 queries and complaints in 2018, as well as 89,271 data breach notifications, both up significantly over 2017. (Note, however, that GDPR was only in force as of May 25, 2018, so the numbers are not strictly comparable.) While 63 percent of these cases had been closed, some 37 percent were still being processed as of May 2019, while 0.1 percent were being appealed—including those (such as the Google case noted in the question) that had led to the supervisory authorities levying some \$60 million in fines in the 7 months following GDPR’s entry into force.

I have not yet seen an analysis of precisely how many of these queries and complaints specifically related to data collection and use standards, although suspect these issues were raised in most of them.

In general, however, I would “grade” the European Union’s enforcement efforts fairly favorably. All EU member states had data protection laws and data protection authorities under the previous 1995 Data Protection Directive, so GDPR was not completely new. That said, the political context surrounding and the emphasis on data protection has increased immensely during the past few years, not least because of the 2013 Snowden revelations and the Cambridge Analytica stories.

This, plus the more detailed and stringent GDPR requirements, places significant demands on the Supervisory Authorities, many of which had to be legally reconstituted to meet GDPR requirements for independence and enforcement authorities. GDPR requires member state governments to provide the requisite resources to the Supervisory Authorities, but this takes time, as does finding sufficient qualified staff (in competition with the private sector compliance business). Even with the 2 years between enactment in April 2016 and entry into force in May 2018, many supervisory authorities, especially in smaller member states, are still struggling to staff up.

They are not helped by the fact that the EDPB is still developing detailed guidance on some of the trickiest parts of GDPR (*e.g.*, on big data analytics, beyond profiling and automated decision-making), and that very little has yet been subjected to detailed judicial review.

These “growing pains” should have been expected, and as noted the majority of Supervisory Authorities are managing them in part by focusing on helping the firms they supervise comply with the GDPR. This necessarily means emphasizing some of the risk and harm-based approaches that are reflected in the GDPR, as implicit in the Data Protection Impact Assessments. Applying such “prosecutorial discretion” makes sense at this point in the GDPR’s life, although those who emphasize the “fundamental right” of data protection may be somewhat disappointed.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ
MASTO FROM PETER H. CHASE**

Data Minimization vs. Big Data

Q.1. Data minimization seeks for businesses to collect, process, and store the minimum amount of data that is necessary to carry out the purposes for which it was collected. There are obvious advantages to this as it minimizes the risk of data breaches and other privacy harms. At the same time, big data analytics are going to be crucial for the future and play an important role in smart cities, artificial intelligence, and other important technologies that fuel economic growth.

Can you describe how you view a balance between minimization and big data? Please describe how this balance applies specifically to the financial sector?

A.1. Data minimization and big data analytics are two different concepts.

The European Union’s General Data Protection Directive (GDPR) requires a data controller (including financial firms) to collect and process personal data in accordance with a number of principles, including the data minimization principle. This requirement in Article 5(1)(c) does not in itself restrict the amount of personal data a controller may collect; it merely stipulates that the data must be “adequate, relevant and necessary in relation to the purposes for which they (the personal data) are processed.”

“Big data analytics”—that is, the application of powerful computing capabilities to large amounts of data to try to determine and learn from certain correlations—*could be* one of the purposes for which a data controller (including a financial firm) collects/processes personal data; that is, GDPR and the data minimization principle do not preclude big data analytics.

That said, under GDPR a controller must also ensure that any processing of personal data complies with other key principles and requirements, including importantly the “lawfulness, fairness and transparency” principle in Article 5(1)(a) and the “purpose limitation” principle in Article 5(1)(b). The first of these requires inter alia that any processing of personal data must be done in accordance with one of the six lawful purposes spelled out in Article 6, while the second mandates that data must be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.”

Many see this “purpose limitation” principle as potentially more problematic for big data analytics than the “data minimization” principle, as a data controller (including a financial firm) might wish to apply such analytics to personal data in a way that was not clearly and specifically envisioned and spelled out to a data subject when the data was collected. Interestingly, neither the European Data Protection Board (EDPB) or its predecessor, the “Working Party 29” (WP-29), have provided clear guidance on this issue.

They have, however, provided detailed guidance (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053) on two of the main purposes for which big data analytics might be applied to personal data, automated decisionmaking and profiling,

both of which are specifically addressed as well in Article 22 of GDPR (<https://gdpr-info.eu/art-22-gdpr/>). The EDPB Guidance notes that both analytical tools may have useful applications, including in financial service industries, and indeed cites financial service applications in a number of the examples. Profiling is defined as:

a procedure which may involve a series of statistical deductions . . . used to make predictions (or evaluations) about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.

Automated decisionmaking can be based on data provided directly by a consumer, observed about that person, or derived or inferred about them; it may or may not involve profiling.

Both of these “big data” procedures are allowable under GDPR, but they must comply the relevant provisions thereof. This may be difficult. Consent may not apply unless the individual was specifically alerted to the specific additional processing to which his or her data might be subjected, and even then the controller needs to meet the requirement that the “consent” also meet the “fairness” principle (including the individual’s reasonable expectations about the use of his/her data). European officials also point to the possibility of using the “legitimate interests” of the controller as a basis for big data analytics, although if so doing a controller would need to demonstrate—probably through a Data Protection Impact Assessment—that the rights of the individuals’ whose data is being processed do not over-rule those interests. The Guidance suggests this will be increasingly difficult to demonstrate the more detailed, comprehensive and impactful the profiling might be for an individual.

Note that under GDPR, an individual has an absolute right to object to the use of profiling for direct marketing purposes.

Security Standards

Q.2. Are the existing data security standards under GLBA sufficient for protecting consumer’s information? If not, what do you recommend to make the standards adequate?

A.2. I do not know enough about the security standards under GLBA to assess whether or not they are sufficient for protecting consumers’ information. The GDPR also has provisions in Articles 32–34 about data security and breach notification, but I am not in a position to compare those with GLBA. Data breaches of course continue to happen in the European Union; the European Union is trying to address these more through the upgrading of its cybersecurity law and regulation than through GDPR.

Discrimination in AI

Q.3. Machine Learning and Artificial Intelligence can often lead to discriminatory and biased outcomes. It is important that Congress address and prevent discrimination in any future privacy legislation.

Q.3.a. Can impact assessments in the financial sector be useful?

A.3.a. Machine Learning and Artificial Intelligence are types of big data analytics, so many of the comments made in response to the first question are also applicable here.

As a general matter, the GDPR's lawfulness and fairness principle would preclude decisionmaking based on personal information that either was not in compliance with existing laws against such discrimination or otherwise unfairly discriminated against an individual.

Data Protection Impact Assessments, as described in detail in GDPR Article 35 (<https://gdpr-info.eu/art-35-gdpr/>) as well as relevant EDPB Guidance (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236), would of course be a useful tool financial service firms could use to determine whether their use of big data analytics, including machine learning and artificial intelligence, is consistent with data protection laws and requirements.

Q.3.b. How do we balance the need for transparency in automated decisionmaking with proprietary business information?

A.3.b. The principle of transparency in automated decisionmaking need not conflict with protecting proprietary business information, an issue discussed in GDPR Recital 63. The EDPB has issued detailed guidance (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227) on this issue, which essentially says that (a) data subjects have a right to access (and rectify) the personal data about them used in automated decisionmaking, and that (b) data controllers need to be able to explain in some detail about how their automated decisionmaking processes work, but do not need to reveal proprietary business data as part of that.¹

Note that the EDPB argues that GDPR prohibits solely automated decisionmaking that has a legal or "similarly significant" effects on an individual, unless in the performance of a contract (where the use of the procedure is clearly spelled out), pursuant to law or with the explicit consent of the individual. Every individual at the least has a right to human intervention in the decision-making and an explanation of the grounds for the decision.

Q.3.c. Where do you think we must be careful to avoid discrimination based on machine learning, AI and other algorithms?

A.3.c. The United States has laws against discrimination, including specific types of discrimination that might be practiced by financial firms, whether or not that discrimination is a result of the use of machine-learning, AI or other algorithms. The existence or not of a general data protection law in the United States along the lines of GDPR does not in any way excuse these firms from their need to obey these laws. The many levels of Government responsible for the enforcement of these laws, however, need to have the appropriate capacity, technical competence and resources to be able to do so in the context of the use of computer-based decisionmaking mechanisms.

Q.3.d. Are you aware of pricing differences for consumer financial products such as loans or credit cards based on algorithms?

¹ See especially the Guidance on Automated Decision Making, page 25 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053).

A.3.d. Personally, no, but differential pricing is both common and permissible in many industries, and specifically financial industries. The use of computer-based analysis/modeling (algorithms) in making these pricing determinations is not novel, and, as noted above, is subject to existing laws.

Q.3.e. Are there firms that you think are utilizing algorithms to expand access for affordable credit or useful financial products that we can learn from?

A.3.e. I am not personally aware of any such firms in the United States or Europe, although have read about ways in which “fintech” is arguably expanding the pool of individuals able to access financial resources.

Harms

Q.4. It is well documented that some businesses have collected and used personal information to engage in digital redlining against marginalized communities in areas from credit to housing to employment and education. Others have sold customer location data intended to help 911 services save lives to bounty hunters, threatening the physical safety of citizens and discredit the use of emergency mechanisms. Data harms, in sum, can be varied and very real, going well beyond narrow financial harms that many would only like to focus on.

What do you believe are the harms Congress should address in privacy legislation aimed at the Nation’s financial sector?

A.4. I am not qualified to respond to the question, specifically with respect to the financial sector, but would not again that all existing laws apply.

I would add that Privacy International has filed complaints under GDPR to the UK’s Information Commissioner’s Office about a number of specific data practices used by data brokers and credit rating agencies that might go to some novel personal data protection issues not now covered by U.S. law.

Impact of GLBA

Q.5. Recent polling found that 94 percent of Californians think that companies should get your permission before sharing your data with third parties. This polling is likely reflective of consumer sentiment across the Nation.

Q.5.a. How many consumers typically take advantage of their right to opt-out of the sale of their data to third parties?

A.5.a. I have not yet seen any data about the number of Europeans who have opted-out of (objected to) the sale of their data to third parties since the GDPR went into force in May 2018. The GDPR (which is more of an “opt-in” approach) does however require that consumers be told in advance how their data will be collected and the specific purposes for which it will be used, and that they have the right to object to the sharing of their data with third parties. This is true even when the data is not provided directly by them (as addressed in Article 13, <https://gdpr-info.eu/art-13-gdpr/>), but also when it has been collected indirectly (Article 14, <https://gdpr-info.eu/art-14-gdpr/>).

Q.5.b. Do you see differences in opt-out options based on firm size? Are consumers more likely to accept tracking from large monopolies like Google, Amazon or Facebook and deny it from smaller sites like local newspapers?

A.5.b. I am not aware of any specific research on this subject, whether related to the United States or in Europe.

National Rules and Standards

Q.6. A lot of data processing is done by third-party processing companies which exist simply to process the data on behalf of any business. They don't necessarily have a say in how the data is used, they simply perform the processing functions for someone else. This is important for a couple reasons. First, it presents a challenge in trying to craft rules because these entities have no consumer facing side. But it also raises the question of how these entities should manage compliance with different data privacy and security laws as they process for businesses that work in different sectors.

What should Congress keep in mind as a few committees of jurisdiction are looking at the data privacy issues with regards to ensuring processors are able to comply with the strong standards we need to set?

A.6. The GDPR, which provides generally applicable rules with respect to the protection of personal data (that is, regardless of sector), distinguishes between data "controllers" and data "processors" for the reason described in the question. The roles and responsibilities of the two are discussed in GDPR Chapter 4, and specifically Articles 24 (Responsibility of the Controller), 26 (Joint Controllers), 28 (Processors) and 29 (Processing under the Authority of the Controller or Processor). In principle, the controllers have the primary responsibility for ensuring that the companies they engage as processors also comply fully with the terms of GDPR. Precisely because the relationship between the controller and the processor can be complex, the EDPB and its predecessor, the WP-29, have provided a number of guidance documents on this, including with respect to the contractual rules that should govern the relationship between them as well as for identifying the "lead supervisory authority" that oversees the relationship.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM JAY CLINE

Q.1. As companies change the way they do business to comply with GDPR in Europe, here in the United States those same companies are voluntarily rolling out the same protections. For example, in April 2018, Facebook announced that it would provide GDPR privacy controls to all its users. My concern is that smaller companies and startups will not be able to voluntarily offer GDPR protections to Americans. What can be done to assist those companies that would like to comply but lack the resources?

A.1. My experience is primarily with large corporations, and I do not have an informed perspective about smaller companies.

Q.2. Is it realistic for the United States to “free-ride” on GDPR? Can we expect companies to voluntarily adopt all or part of GDPR? How can we avoid a balkanized world of privacy regulations?

A.2. I have published an analysis of the world’s privacy regulations, highlighting the areas where there are common agreement and the areas where there are divergence. I advise companies to build global privacy capabilities in areas where there is common agreement—such as employee training and incident response—and local capabilities where there are divergence, such as on individual rights.

Q.3. As consumers begin to demand additional privacy protections, we will undoubtedly hear pushback from U.S. firms that too much regulation will undermine our competitive edge. According to analyses by Goldman Sachs, Facebook’s revenue could “potentially see a negative impact of up to 7 percent from GDPR.” In your experience, are these concerns founded? And how can we strike a balance that protects consumers while allowing firms to grow?

A.3. There are indeed administrative requirements of GDPR which impose commercial burdens without providing obvious, concrete improvements in consumer privacy from an American perspective. For example, requirements to document cross border data-transfer agreements and document the legal basis of data processing are vestiges of Europe’s unique approach to data privacy. The widespread adoption by websites of cookie pop-up boxes in GDPR’s wake are another example of administrative steps that do not practically improve consumer privacy.

Some of the major requirements of the GDPR, however, have North American origins, such as the data-breach notification rules that emanate from the United States, and Privacy by Design that originates from Canada. Other parts of the GDPR—such as data inventorying and risk assessments—reflect a code of good business practice that I have long advised clients to undertake in order to achieve their business objectives and protect their brands.

The American-led rise of social media and mobile phones has both given the United States a global economic competitive advantage and shown American consumers are willing to trust these technologies while also demanding higher privacy protections. The sharp rise this year in venture-capital-funded, innovative U.S. privacy technologies that sell their products to large enterprises reflects a market expectation that American consumers will continue to demand an increasing level of privacy protection in the years ahead.

I advise clients to strike this balance between protection and innovation by designing a data architecture that puts consumers in control of their personal data, protecting that data throughout its lifecycle, and resolving privacy and ethical impact assessments for all new business and technology change. I have found that companies that take this approach achieve a more complete view of their data for innovation purposes, and also earn more trust of their stakeholders.

Q.4. We are approaching the 1-year anniversary of the GDPR. What are some of the negative unintended consequences that the

United States can learn from as Congress explores its own privacy legislation?

A.4. One study¹ of new deals activity in the European Union showed a decrease after GDPR's go-live date of May 2018. This study matched anecdotal evidence that investors perceived higher risk and uncertainties in the European Union, particularly with regard to the potential of a corporation to be fined 4 percent of its annual revenues for egregious violations of the GDPR. The July 2019 GDPR enforcement actions by the U.K. Information Commissioner that established record privacy fines in the European Union reinforced the perception that this fining capacity represents material risk for investors in the EU market.

Q.5. A central element of GDPR is that companies must clearly explain how data is collected and used. Already we've seen companies such as Google face heavy fines for failing to comply with GDPR's consent requirements. How would you grade the European Union's enforcement of GDPR standards writ large, but also specifically the data collection and use standards?

A.5. Many industry observers expected EU member states' first wave of privacy investigations to conclude sooner than they have. Since the hearing in May 2019, the United Kingdom has indicated its intention to impose the two largest privacy fines in EU history. It remains to be seen what the European Union's steady state of GDPR enforcement will be.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ
MASTO FROM JAY CLINE**

Data Minimization vs. Big Data

Q.1. Data minimization seeks for businesses to collect, process, and store the minimum amount of data that is necessary to carry out the purposes for which it was collected. There are obvious advantages to this as it minimizes the risk of data breaches and other privacy harms. At the same time, big data analytics are going to be crucial for the future and play an important role in smart cities, artificial intelligence, and other important technologies that fuel economic growth.

Can you describe how you view a balance between minimization and big data? Please describe how this balance applies specifically to the financial sector?

A.1. The tremendous potential of big data can be achieved only with the ongoing trust of the people whose data are used for these purposes. Two components of gaining that trust ordinarily are transparency and individual control. People generally want to know how their data will be used in large-scale data sets, and they want the ability to not participate if they disagree with the uses. In order to deliver these two components of transparency and individual control, organizations would need to implement a new "data architecture." Today, most companies organize their technology around a "systems architecture" that connects servers to each other

¹ <https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/>.

in a network. To enable a single individual to remove their data from the entire network without causing individual applications and databases to stop working, however, and to make sure data was minimized to the agreed-upon purposes, companies would need to engineer their systems at a more granular, data-element level. Achieving a balance between data minimization and big data can be done, but it requires a re-thinking about how information technology is organized.

Security Standards

Q.2. Are the existing data security standards under GLBA sufficient for protecting consumer's information? If not, what do you recommend to make the standards adequate?

A.2. The most important and effective standard of the GLBA Safeguards Rule and how it has been enforced by the Federal Trade Commission is the requirement to regularly assess vulnerabilities and to remediate material vulnerabilities with commercially reasonable and available means. This all-encompassing approach—if implemented consistently and comprehensively across an organization—should result in substantial and ongoing protection of consumer information from unauthorized access or disclosure. NIST has similarly developed useful and effective information security standards that when implemented have elevated the protection of consumer information.

Discrimination in AI

Q.3. Machine Learning and Artificial Intelligence can often lead to discriminatory and biased outcomes. It is important that Congress address and prevent discrimination in any future privacy legislation.

Q.3.a. Can impact assessments in the financial sector be useful?

A.3.a. Privacy impact assessments with supplemental data-ethics criteria can be useful and practically essential in meeting the objective of eliminating bias in machine learning and artificial intelligence. In the same way that software applications are tested before they are put into production, algorithms that an impact assessment determines could cause substantially negative and disparate outcomes on vulnerable populations can be evaluated and improved before deployment.

Q.3.b. How do we balance the need for transparency in automated decisionmaking with proprietary business information?

A.3.b. Most automated decisionmaking programs are designed around three components: data input, data processing, and data output. The data input and the data output components are the most important to make transparent to people whose data are being processed in order for them to make informed decisions about whether they want their data included. Protecting the confidentiality of the middle, data-processing stage is the most important in order to preserve proprietary secrets. For example, highlighting to a user that they may like to buy a certain product because they bought a past product that others like them purchased demonstrates the relationship between the input and the output without revealing the business secret of why the one product

recommendation topped all of the other options. From a regulatory standpoint, GDPR article 15 contains a right of access to “meaningful information about the logic involved” in automated decision-making. This threshold falls short of requiring companies to provide their confidential source code as part of an access request.

Q.3.c. Where do you think we must be careful to avoid discrimination based on machine learning, AI and other algorithms?

A.3.c. I am recommending to my clients that they prioritize for privacy and ethical impact assessments any data-analytics processes that could reduce access to the basic necessities of life—food, clothing, housing, credit, insurance, and employment.

Q.3.d. Are you aware of pricing differences for consumer financial products such as loans or credit cards based on algorithms?

A.3.d. I am not aware of these specific scenarios.

Q.3.e. Are there firms that you think are utilizing algorithms to expand access for affordable credit or useful financial products that we can learn from?

A.3.e. I see positive steps taking place in the area of risk scoring within some parts of the financial services sector whereby advanced data analytics reduce uncertainty and allow for the reduction of rates and premiums, creating more access to credit and insurance.

Harms

Q.4. It is well documented that some businesses have collected and used personal information to engage in digital redlining against marginalized communities in areas from credit to housing to employment and education. Others have sold customer location data intended to help 911 services save lives to bounty hunters, threatening the physical safety of citizens and discredit the use of emergency mechanisms. Data harms, in sum, can be varied and very real, going well beyond narrow financial harms that many would only like to focus on.

What do you believe are the harms Congress should address in privacy legislation aimed at the Nation’s financial sector?

A.4. The GDPR includes a principle to use personal data only for the purpose it was originally collected, which has become a generally accepted industry standard in the privacy profession. Companies following this principle will generally avoid causing the aforementioned harms.

Impact of GLBA

Q.5. Recent polling found that 94 percent of Californians think that companies should get your permission before sharing your data with third parties. This polling is likely reflective of consumer sentiment across the Nation.

Q.5.a. How many consumers typically take advantage of their right to opt-out of the sale of their data to third parties?

A.5.a. Consumers’ exercise of any type of opt-out right is highly dependent upon the context. Low, single-digit rates are normally observed if a consumer must log in to a preference center or click a link in an email footer to express a choice. Higher rates are seen

when the opt-out choices are presented prominently during an account sign-up, registration, or reservation. The highest rates are seen when consumers must express one choice or another in order to successfully download a mobile app.

Q.5.b. Do you see differences in opt-out options based on firm size? Are consumers more likely to accept tracking from large monopolies like Google, Amazon or Facebook and deny it from smaller sites like local newspapers?

A.5.b. My experience is primarily with large corporations, and I don't have an informed perspective on this question.

National Rules and Standards

Q.6. A lot of data processing is done by third-party processing companies which exist simply to process the data on behalf of any business. They don't necessarily have a say in how the data is used, they simply perform the processing functions for someone else. This is important for a couple reasons. First, it presents a challenge in trying to craft rules because these entities have no consumer facing side. But it also raises the question of how these entities should manage compliance with different data privacy and security laws as they process for businesses that work in different sectors.

What should Congress keep in mind as a few committees of jurisdiction are looking at the data privacy issues with regards to ensuring processors are able to comply with the strong standards we need to set?

A.6. Data processors face a fundamental challenge that they often do not have direct relationships with the people whose data they process. They act as agents of their clients who they depend on to manage privacy-rights processes with consumers. Their clients in turn are challenged to deploy sufficient monitoring mechanisms to ensure their data processors are only using personal data to fulfill their contractual terms. GDPR addresses this situation by requiring data controllers to hold their data processors accountable to relevant GDPR requirements, while HIPAA holds business associates directly accountable to the relevant provisions of the law. Neither creates specific rules for data processors. Together, these two approaches form the bookends of the current privacy regulatory spectrum regarding data processors.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM MACIEJ CEGLOWSKI

Q.1. What happens to a consumer's data after a consumer terminates their relationship with an institution collecting their data? Does the company delete the consumer's data? Does it encrypt the data?

A.1. Response not received in time for publication.

Q.2. Is there any uniform requirement or industry practice that dictates how institutions treat consumer data once a consumer decides to no longer conduct business with an institution?

A.2. Response not received in time for publication.

Q.3. If company is breached after a consumer has terminated their relationship, is the consumer's data still vulnerable?

A.3. Response not received in time for publication.

Q.4. To ensure consumer data is protected, should consumers be allowed to request their personally identifiable information be made nonpersonally identifiable, after the consumer ends their business relationship?

A.4. Response not received in time for publication.

Q.5. Using the Equifax data breach as an example, how much harm can bad actors, free from consumer scrutiny and armed with sensitive information, cause in 6 weeks?

A.5. Response not received in time for publication.

Q.6. Would consumers be better protected if companies were required to notify them of data breaches in a timely manner?

A.6. Response not received in time for publication.

Q.7. As companies change the way they do business to comply with General Data Protection Regulation (GDPR) in Europe, here in the United States those same companies are voluntarily rolling out the same protections. For example, in April 2018, Facebook announced that it would provide GDPR privacy controls to all its users. My concern is that smaller companies and startups will not be able to voluntarily offer GDPR protections to Americans. What are the implications for smaller businesses that want to comply but don't have the resources to do so?

A.7. Response not received in time for publication.

Q.8. As consumers begin to demand additional privacy protections, we will undoubtedly hear pushback from U.S. firms that too much regulation will undermine our competitive edge. According to analyses by Goldman Sachs, Facebook's revenue could "potentially see a negative impact of up to 7 percent from GDPR." In your experience, are these concerns founded? And how can we strike a balance that protects consumers while allowing firms to grow?

A.8. Response not received in time for publication.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM MACIEJ CEGLOWSKI

Data Minimization vs. Big Data

Q.1. Data minimization seeks for businesses to collect, process, and store the minimum amount of data that is necessary to carry out the purposes for which it was collected. There are obvious advantages to this as it minimizes the risk of data breaches and other privacy harms. At the same time, big data analytics are going to be crucial for the future and play an important role in smart cities, artificial intelligence, and other important technologies that fuel economic growth.

Can you describe how you view a balance between minimization and big data? Please describe how this balance applies specifically to the financial sector?

A.1. Response not received in time for publication.

Security Standards

Q.2. Are the existing data security standards under GLBA sufficient for protecting consumer's information? If not, what do you recommend to make the standards adequate?

A.2. Response not received in time for publication.

Discrimination in AI

Q.3. Machine Learning and Artificial Intelligence can often lead to discriminatory and biased outcomes. It is important that Congress address and prevent discrimination in any future privacy legislation.

Q.3.a. Can impact assessments in the financial sector be useful?

A.3.a. Response not received in time for publication.

Q.3.b. How do we balance the need for transparency in automated decisionmaking with proprietary business information?

A.3.b. Response not received in time for publication.

Q.3.c. Where do you think we must be careful to avoid discrimination based on machine learning, AI and other algorithms?

A.3.c. Response not received in time for publication.

Q.3.d. Are you aware of pricing differences for consumer financial products such as loans or credit cards based on algorithms?

A.3.d. Response not received in time for publication.

Q.3.e. Are there firms that you think are utilizing algorithms to expand access for affordable credit or useful financial products that we can learn from?

A.3.e. Response not received in time for publication.

Harms

Q.4. It is well documented that some businesses have collected and used personal information to engage in digital redlining against marginalized communities in areas from credit to housing to employment and education. Others have sold customer location data intended to help 911 services save lives to bounty hunters, threatening the physical safety of citizens and discredit the use of emergency mechanisms. Data harms, in sum, can be varied and very real, going well beyond narrow financial harms that many would only like to focus on.

What do you believe are the harms Congress should address in privacy legislation aimed at the Nation's financial sector?

A.4. Response not received in time for publication.

Impact of GLBA

Q.5. Recent polling found that 94 percent of Californians think that companies should get your permission before sharing your data with third parties. This polling is likely reflective of consumer sentiment across the Nation.

Q.5.a. How many consumers typically take advantage of their right to opt-out of the sale of their data to third parties?

A.5.a. Response not received in time for publication.

Q.5.b. Do you see differences in opt-out options based on firm size? Are consumers more likely to accept tracking from large monopolies like Google, Amazon or Facebook and deny it from smaller sites like local newspapers?

A.5.b. Response not received in time for publication.

National Rules and Standards

Q.6. A lot of data processing is done by third-party processing companies which exist simply to process the data on behalf of any business. They don't necessarily have a say in how the data is used, they simply perform the processing functions for someone else. This is important for a couple reasons. First, it presents a challenge in trying to craft rules because these entities have no consumer facing side. But it also raises the question of how these entities should manage compliance with different data privacy and security laws as they process for businesses that work in different sectors.

What should Congress keep in mind as a few committees of jurisdiction are looking at the data privacy issues with regards to ensuring processors are able to comply with the strong standards we need to set?

A.6. Response not received in time for publication.

Data Protection Officers

Q.7. In your testimony, you note the lack of qualified data protection officers.

- What are the qualifications for a data protection officer (DPO)?
- What are the costs for a firm to hire and train a DPO?
- What training exists for DPOs? How are they certified? What is the cost for a DPO to attain certification? Do the salaries paid to DPOs allow them to repay their student loans and also support themselves and their families?

A.7. Response not received in time for publication.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD



Statement for the Record

Submitted to the

U.S. Senate Banking, Housing and Urban Affairs Committee

"Privacy Rights and Data Collection in a Digital Economy"

May 7, 2019

On Behalf of

Susan K. Neely
President and CEO
The American Council of Life Insurers

The American Council of Life Insurers (ACLI) appreciates the opportunity to submit this statement for the record on "Privacy Rights and Data Collection in a Digital Economy."

ACLI is the leading trade association driving public policy and advocacy on behalf of the life insurance industry and the 90 million American families relying on life insurers' products for financial protection and retirement security. ACLI's 280 member companies represent 95 percent of industry assets and are dedicated to promoting consumers' financial well-being with products that reduce risk and increase their financial security, including life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, dental and vision insurance and other supplemental benefits. The core business of the life insurance industry is financial security, and retirement security is a critical mission. As society and work change, the industry is committed to solutions that protect all Americans, regardless of where and how they work, their life stage, or the economic status of their household. Life insurers seek to expand the availability, accessibility, and affordability of financial protection and retirement security products for all.

Life insurance customers have the right to expect their personal information will be kept confidential and secure by life insurers. The life insurance industry has long been a diligent steward of personal information. Our member companies have appropriately managed consumers' sensitive medical and financial information far before it became "data" and was monetized by the tech sector. While the use of data is a "Wild West" on the tech side, with little protection and oversight, the financial service industry has robust regimen for the use of data. Many of the items in these proposals aimed at protecting consumers' personal information are our common practices. We hope that our industry's record of responsible stewardship of consumer information can serve as a model to policy makers as they seek to protect consumers in other areas. The life insurance industry affirmatively supports consumer transparency and control over the use of their personal information.

Life insurers collect, use, and disclose the use of customers' personal information to perform essential life insurance business functions. Examples of this use include underwriting applications for new life, disability income, and long-term care insurance policies and paying claims submitted under these policies. At the same time, our industry is subject to a broad and rigorous regulatory framework at both the state and federal level, that requires life insurers to protect their customers' personal information. While we support this framework of laws and regulations, we recognize that in this period of rapid technological advancement a new approach may be needed to comport with today's increasingly cyber world. As Congress works to develop a new privacy regulatory structure, we ask that policymakers call upon the expertise of the life insurance industry with regard to the privacy of customer and consumer information.

Life insurance companies also have robust data security programs in recognition of their affirmative obligation to protect the security of their customers' personal information and the information systems on which such information is stored. The life insurance industry supports uniform, clear, and reasonable data security standards and breach notification requirements. We act as responsible stewards entrusted with safeguarding the data and are required to comply with federal laws such as Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), and Health Insurance Portability and Accountability Act (HIPAA). We use security

measures that comply with federal law to protect our customers' personal information from unauthorized access and use.

We are hopeful that as the Senate Banking Committee considers the important and complex issues related to privacy and security, Members continue to keep in mind:

- life insurers' need to collect and use consumers' personal information to perform fundamental insurance business functions;
- the current privacy and data security framework to which life insurers are already subject; and
- the need for uniformity across regulatory platforms so that life insurers can continue to effectively and efficiently protect the privacy and security of their customers' personal information.

Again, thank you for the opportunity to comment on these important issues, and we look forward to working with you as your deliberations continue.



HELPING FINANCE THE AMERICAN DREAM SINCE 1919.

May 7, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
U.S. Senate
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
U.S. Senate
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the Consumer Bankers Association (CBA), I write to share our views on a national data privacy framework for the Senate Banking, Housing, and Urban Affairs Committee's hearing entitled "Privacy Rights and Data Collection in a Digital Economy." CBA is the voice of the retail banking industry whose products and services provide access to credit for consumers and small businesses. Our members operate in all 50 states, serve more than 150 million Americans, and collectively hold two-thirds of the country's total depository assets.

The State of Data Privacy

In light of recent data breaches and abuses, consumers are rightly concerned about the manner in which their personal information is being collected and how this sensitive information is being both shared and protected. In 2018 alone, the number of data breaches in the U.S. totaled more than 1,200 according to the Identity Theft Resource Center. No industry was immune from breaches in 2018: business sector (46 percent), healthcare/medical industry (29 percent), banking/credit/financial industry (11 percent), government/military (8 percent), and the education sector (6 percent). However, it is important to note that the non-financial business sector, which is not subject to national data security requirements, was responsible for the overwhelming majority (93 percent) of the personal records compromised. In addition to breaches, there have been several noteworthy examples of misuse of customer data in the past year which warrant a review of industry practices and the scope of federal privacy laws and regulations, e.g. Cambridge Analytica gained access to private information on more than 50 million Facebook users.¹

CBA members take seriously their responsibility to clearly explain the uses of consumers' data and to safeguard it against improper use and criminals attempting to steal it. Since the passage of the Gramm-Leach-Bliley Act (GLBA) in 1999, financial institutions have been required to provide their customers a clear privacy notice detailing information collection and sharing practices, which includes an opt-out for the sharing of information with non-affiliated third parties. This notice is provided at the beginning of the customer relationship and annually thereafter. GLBA and subsequent regulations also require banks to have in place data security protocols to safeguard sensitive consumer information and to report to federal authorities and affected consumers when a breach occurs. Banks are examined by their prudential regulators on these standards and if found to be non-compliant may face fines or other penalties.

The low breach-rate of personally identifiable information (PII) at financial institutions compared to other sectors can be attributed to the common-sense safeguards required by GLBA and the industry's commitment to security. As a

¹ <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

result, consumers trust financial institutions more than any other type of organization to keep their financial information secure, according to an August 2017 poll by Morning Consult.

Consumer Privacy

CBA supports consumers having reasonable control concerning the collection, use and sharing of personal data. However, we caution against national privacy legislation that may inhibit banks' ability to fulfill their contractual obligations to consumers. Compared to other industries, banks are subject to more stringent rules and lead in protecting consumers' PII and their privacy.

Pursuant to the GLBA, banks are required to protect the security and confidentiality of consumer records and information, and the law also requires banks to disclose their privacy practices and limits sharing PII with nonaffiliated third parties. Any Federal privacy law must consider the GLBA and other existing Federal privacy laws and preempt the growing patchwork of state laws that provide differing and inconsistent consumer protections. Otherwise, a consumer's privacy protections, including their ability to understand their rights, will depend on the state where the individual resides. While these state laws may be well-intentioned, they must be crafted to not hinder the free flow of data needed to provide consumers and businesses with financial products and services and process financial transactions.

As Congress considers the creation of a national data privacy framework, we must first recognize the differences in data collection among industries. Banks are required by federal law to collect certain information to conduct a customer transaction. For example, if a consumer wants to open a checking account, at a minimum pursuant to the Bank Secrecy Act, the bank must obtain certain information to fulfill its Customer Identification Program requirements, such as date of birth, address, and identification number. As an additional benefit to customers, banks also use personal data to develop banking products and services that are customized to a customer's needs. Utilizing consumer data to conduct financial transactions authorized by the consumer is far different than a social media platform collecting consumer data to sell to marketers.

It is also important that a federal privacy standard should not expand the scope of data that banks are responsible for protecting. GLBA requires banks to protect consumers "nonpublic personal information", which is defined, in part, as "[...] personally identifiable financial information, (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."² Consumer is defined to mean "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personally, family, or household purposes, or that individual's legal representative."³ An expansion of the definition of covered data or covered persons pursuant to a national standard would subject banks to unnecessary regulatory burden.

A national data protection and privacy law must also seek to promote innovation, investment and competition in the marketplace. The United States Constitution authorizes Congress to regulate interstate commerce, which includes the free flow of goods, services and consumer data. A patchwork of privacy laws at the state level will lead to higher costs for consumers and create barriers to innovation and investment. The assumption that preemption weakens existing state laws is a fallacy. In a world that is increasingly mobile, Americans and their devices constantly cross state borders. Consumer protection should not depend upon which state you reside, but consumers should be covered by one unified, comprehensive federal standard.

² https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=15-USC-697127498-1137964384&term_occur=2&term_src=title:15:chapter:94:subchapter:1:section:6801

³ https://www.law.cornell.edu/uscode/text/15/6809#4_A

From an international perspective, CBA also supports an open global economy that enables growth through the secure and efficient transfer of data across international borders. National data protection and privacy legislation should continue to support consumer privacy while also respecting and coordinating differences between U.S. and foreign privacy regimes.

National data protection and privacy legislation should be enforced by the Federal Trade Commission (FTC), unless a determination is made that it is appropriate for a different regulator to be the enforcement agency, e.g. prudential regulators for banks and credit unions. CBA is concerned that if state attorneys general are allowed to bring enforcement actions in federal court, there is a risk that each state will enforce the law differently. In addition, a national consumer privacy law should not provide for a private right of action.

Lastly, the California Consumer Privacy Act is the first major consumer privacy law to be adopted at the state level. This legislation was written hastily, and the state government is currently reviewing and revising portions of the law through both legislative and regulatory processes. As the California privacy law continues to evolve, it would be prudent for Congress to monitor issues with implementation and use their observations to draft a federal data privacy and security standard. Considering the importance of this issue and the impact it will have on both consumers and businesses, it is imperative that Congress is thoughtful in drafting meaningful legislation to protect consumers and provide businesses with certainty.

Data Security and Breach Notification

It is also critical that any conversation around data privacy also take seriously the security of data and the protocol for notifying customers in the event of a breach. Banks are on the front lines consistently monitoring for fraud and working to make consumers whole, no matter where a breach occurs. From operating advanced fraud monitoring systems to reissuing cards, CBA members spend considerable resources on preventing fraud. As a result, consumers rely on their financial institutions to communicate what to do in the event of a breach and to employ defenses to prevent fraud and identity theft.

Subsequent to Section 501(b) of GLBA, the financial regulators issued guidelines requiring banks to implement comprehensive, risk-based information security programs that include administrative, technical and physical safeguards to protect customer information. These safeguards are not static but flexible and scalable – applying to banks of all sizes. A similar framework should be applied to non-bank companies to ensure consumers' sensitive information is protected throughout the payment system.

Banks must also implement a risk-based response program in the event of a breach. The program includes an evaluation of the incident and an effort to prevent further unauthorized access as well as notice to the institution's primary federal regulator, appropriate law enforcement, and, importantly, the customers whose information was breached and could be misused. CBA supports legislation to require others in the payment system to provide timely notification to their customers in the event of a breach.

Today, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of a security breach of information involving PII.⁴ Twenty-four states currently have data security laws requiring a level of security procedures and practices to be in place to protect personal information.⁵

⁴ <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

⁵ <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>

Congress has the constitutional authority to regulate interstate commerce through the Commerce Clause, which was written to prevent fragmentation of markets and to encourage the free flow of goods and services, including information, across the nation with minimal interference. Congress should take seriously its authority and enact a federal data security and breach notification standard and preempt the current patchwork of state laws. With the recent breaches that have put millions of consumers at risk, the need to pass legislation to establish such a standard could not be more evident. Protecting consumer information is a shared responsibility of all parties involved.

On behalf of our members, I would like to thank you for your consideration of our views. We look forward to working with the Committee to foster an environment that prioritizes the protection and privacy of consumer data while promoting consumer access to credit.

Sincerely,

A handwritten signature in cursive script, appearing to read "Rich. Hunt".

Richard Hunt
President and CEO
Consumer Bankers Association



Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

99 M Street SE
Suite 300
Washington, DC 20003-3799

May 7, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing and Urban
Affairs
United States Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing, and Urban
Affairs
United States Senate
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown,

On behalf of America's credit unions, thank you for holding the hearing on "Privacy Rights and Data Collection in a Digital Economy." The Credit Union National Association (CUNA) represents America's credit unions and their 115 million members.

We applaud the committee for taking up the critical issue of data privacy and we pledge to work with you to create a strong, national data privacy standard. It should go without saying that any serious data privacy statute should include robust data security requirements that all who hold consumer data must follow. Unfortunately, as we have watched the debate over a federal data privacy standard develop, discussion of security requirements has been virtually nonexistent. Nevertheless, we do not see any way for a data privacy law to achieve its objectives without a strong security standard that is preemptive of state law and applies to all entities that hold or use consumer data. Simply put: Congress cannot provide consumer with data privacy without addressing data security.

Congress Should Treat Data Privacy as a National Security Issue

Since 2005, there have been more than 10,000 data breaches in the United States, compromising nearly 12 billion consumer records. These breaches are no longer just the work of lone domestic hackers. Time and time again, we learn that these breaches are being perpetrated by foreign governments, domestic organized crime syndicates and rogue international actors that use the data to help fund their illicit activity. We urge the Committee to treat this issue for what it is: a national security issue.

Congress Should Fix the Weak Links in the System

If Congress is serious about protecting the privacy of consumers' data, then the guiding principle should focus on fixing the weak links that these criminals exploit. In this case, the weak link is that the entities that hold and use consumer data are not all subject to federal data security requirements. Financial institutions and health care providers have long been subject to federal laws that protect the use and security of consumers' and patients' information. These laws, the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act respectively, require financial institutions, including credit unions, and healthcare service providers to have robust privacy and data security protections to protect and control the use of consumer and patients' data that they collect and house as necessary to provide essential services to Americans.

The privacy regulations required by the GLBA were originally promulgated by each financial institutions' regulator. This authority was transferred to the Consumer Financial Protection Bureau (CFPB) with the signing of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. The CFPB's privacy regulation requires that banks and credit unions provide an annual privacy notice to consumers, limits the sharing of information and allows consumers to opt-out of the limited sharing that is allowed. Credit unions and banks are also examined by federal and state regulators for compliance with privacy and data security laws.

cuna.org

There is a reason we have not seen widespread data breaches in the financial services sector as we have seen in other sectors: GLBA, although not perfect, has worked well and helped to solidify credit unions' and banks' long history of safeguarding information. It is long past time for all entities that hold or use consumer data to be subject to federal data security standards.

Congress Should Set a Strong Federal Standard that Preempts State Laws

With that vast amounts of data that businesses now collect with and without consumers' permission and/or knowledge, informed consent and even awareness of data collection and use becomes confusing for consumers. States are now stepping in to fill gaps to ensure consumers are protected when any business collects, uses or houses their information.¹ Although state privacy regulations can help consumers, they will also result in a patchwork of protections that will vary from state to state and likely result in many different privacy and data security requirements. A hodgepodge of state requirements will provide uneven protection for consumers and expensive compliance for businesses.

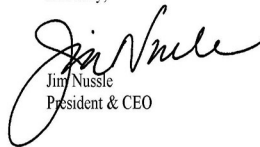
The best approach for consumers and business moving forward is for Congress to develop a strong privacy law that applies to all businesses and entities that collect, house or otherwise possess information. We urge you to take the best of state data security law, make it the federal standard and apply it to everyone. This will ensure efficiency for businesses and strong, consistent protections for consumers.

Conclusion

There is an urgent need for Congress to act to set a federal data privacy standard. The American consumer is under attack and current federal law leaves the door open for criminals, terrorist organizations and foreign governments to steal payment and other personally identifiable information to the benefit of their illicit activity. Taking a narrow view that this debate is about Facebook, Amazon and Google would be a grave mistake. There is no way for Congress to provide consumers with the data privacy they need without enacting robust data security standards that are preemptive of state law and apply to everyone.

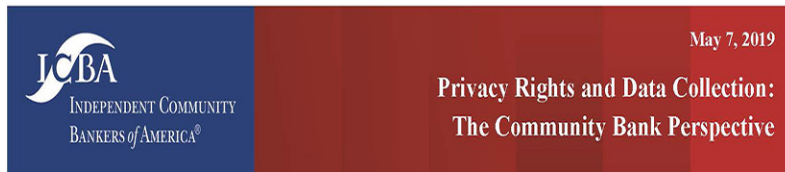
On behalf of America's credit unions and their 115 million members, thank you for your consideration of our views on this important issue.

Sincerely,



Jim Nussle
President & CEO

¹ See the California Consumer Privacy Act (CCPA).



Chairman Crapo, Ranking Member Brown, members of the Committee, the Independent Community Bankers of America, representing community banks across the nation with more than 52,000 locations, appreciates the opportunity to provide this statement for the record in connection with today's hearing on "Privacy Rights and Data Collection in a Digital Economy." ICBA greatly appreciates your opening the discussion of a critical public policy issue that will only become more significant as the digital economy becomes more pervasive.

Community banks are committed to safeguarding consumer data and honoring consumers' preferences in the use of such data. Attached is a comprehensive statement of community banks' policies, practices, and preferences with regard to the collection and use of personally identifiable information ("PII"), which was previously submitted to this committee in response to your request. Below we highlight the principles which will guide our evaluation of any proposed legislation in this area:

- ICBA supports current privacy standards, such as those in the Gramm-Leach-Bliley Act ("GLBA"). To ensure consumers receive enhanced protection of their personal information, all entities that handle personal information should be required to safeguard this information, in a manner comparable to financial institutions.
- A national breach notification standard would be a good first step to ensure consistent consumer notification in the case of a breach, rather than a patchwork of state laws in this area.
- ICBA supports the current privacy notice requirements. Banks are required, through law and regulation, to provide privacy notices and a myriad of disclosures to consumers and customers about the information they collect and share and the purpose of the information.
- Banks are required to collect certain PII based on various regulatory requirements and provide that information to prudential regulators. Prudential regulators must also appropriately safeguard that information.
- Third parties that contract with banks for services which are not currently subject to examination and supervision should also be examined and supervised for their compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Guidelines"), implementing the Gramm-Leach-Bliley Act.
- The credit reporting agencies ("CRAs"), also known as credit bureaus, should be subject to comparable supervision and examination as banks.
- CRAs should focus on educating and informing the consumer about the use of credit reports and their consumer data collection and sharing practices.
- Non-bank entities accessing customer account data must be held responsible for ensuring the security of the consumer information they are accessing and must be held liable for any data breaches and consumer harm which they cause.
- Consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.



ICBA looks forward to providing ongoing input on the impact of proposed legislation concerning the collection and use of personally identifiable information ("PII") on community banks and their customers.

ATTACHMENT: March 14, 2019 ICBA Letter to Chairman Crapo and Ranking Member Brown Regarding Community Banks and Consumer Data

Timothy K. Zimmerman, *Chairman*
 Preston L. Kennedy, *Chairman-Elect*
 Noah W. Wilcox, *Vice Chairman*
 Kathryn Underwood, *Treasurer*
 Christopher Jordan, *Secretary*
 R. Scott Heikamp, *Immediate Past Chairman*
 Rebeca Romero Rainey, *President and CEO*



March 14, 2019

U.S. Senate Committee on Banking, Housing and Urban Affairs
 Chairman Mike Crapo
 Ranking Member Sherrod Brown
 534 Dirksen Senate Office Building
 Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the Independent Community Bankers of America ("ICBA"),¹ I thank you for the opportunity to provide our views about potential legislation in the 116th Congress concerning the collection and use of personally identifiable information ("PII"). We welcome the opportunity to discuss our responses in greater detail. The community banking sector takes seriously the ongoing protection of customers' data and privacy and ICBA advocates for constructive policy changes, specifically:

- ICBA supports current privacy standards, such as those in the Gramm-Leach-Bliley Act ("GLBA"). To ensure consumers receive enhanced protection of their personal information, all entities that handle personal information should be required to safeguard this information, in a manner comparable to financial institutions.

¹ The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. With more than 52,000 locations nationwide, community banks constitute 99 percent of all banks, employ more than 760,000 Americans and are the only physical banking presence in one in five U.S. counties. Holding more than \$4.9 trillion in assets, \$3.9 trillion in deposits, and \$3.4 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities

The Nation's Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org

- A national breach notification standard would be a good first step to ensure consistent consumer notification in the case of a breach, rather than a patchwork of state laws in this area.
- ICBA supports the current privacy notice requirements. Banks are required, through law and regulation, to provide privacy notices and a myriad of disclosures to consumers and customers about the information they collect and share and the purpose of the information.
- Banks are required to collect certain PII based on various regulatory requirements and provide that information to prudential regulators. Prudential regulators must also appropriately safeguard that information.
- Third parties that contract with banks for services which are not currently subject to examination and supervision should also be examined and supervised for their compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Guidelines"), implementing the Gramm-Leach-Bliley Act.² • The credit reporting agencies ("CRAs"), also known as credit bureaus, should be subject to comparable supervision and examination as banks.
- CRAs should focus on educating and informing the consumer about the use of credit reports and their consumer data collection and sharing practices.
- Non-bank entities accessing customer account data must be held responsible for ensuring the security of the consumer information they are accessing and must be held liable for any data breaches and consumer harm which they cause.
- Consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.

Question 1: What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?

Community banks and other financial institutions are required by statute and regulation³ to safeguard personally identifiable information. To ensure consumers receive enhanced protection of their personal information, all entities that handle personal information should be required to safeguard this information, in a manner comparable to financial institutions. With regard to breach notification, a good first step would be to implement a national notification standard, rather than a patchwork of state laws in this area.

Protection of Customer Data

The Nation's Voice for Community Banks.®

WASHINGTON, DC 1615 L Street NW Suite 900 Washington, DC 20036	SAUK CENTRE, MN 518 Lincoln Road PO Box 267 Sauk Centre, MN 56378	866-843-4222 www.icba.org
---	--	------------------------------

By their very nature, community banks and other financial institutions must collect sensitive nonpublic personally-identifiable information (“PII”)⁴ about customers to meet their needs for

² 12 C.F.R. Part 30, Appendix B. and The Financial Modernization Act of 1999, the “Gramm-Leach-Bliley Act,” P.L. 106-102.

³ The Financial Modernization Act of 1999, the “Gramm-Leach-Bliley Act,” P.L. 106-102. The “Interagency Guidelines Establishing Information Security,” 12 C.F.R. Part 30, Appendix B. FFIEC IT Examination Handbook, <https://it handbook.ffiec.gov/>.

⁴ Nonpublic personal information is a term commonly referenced in regulations. Nonpublic personal information is, generally speaking, personally identifiable financial information that is not publicly available. It is also defined as information that is not publicly available and that:

- a consumer provides to a financial institution to obtain a financial product or service from the institution;
- results from the transaction between the consumer and the institution involving service; or a financial product or
- a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

financial services, which includes an array of deposit and loan services. This information is also used to prevent fraud, identity theft and comply with various regulatory requirements.

Safeguarding customer information is central to financial institutions maintaining public trust and retaining customers.

ICBA has consistently advocated that all participants in the payments and financial systems, including merchants, aggregators and other entities with access to customer financial information, should be subject to Gramm-Leach-Bliley Act-like data security standards. Similarly, any entity that processes or holds personally sensitive information about consumers should be required to safeguard that information, just as banks are required. Under current federal law, retailers and other parties that process or store sensitive consumer information are not subject to the same federal data security standards and oversight as financial institutions. Securing personally sensitive data at financial institutions is of limited value if it remains exposed at the point-of-sale and other processing and collecting points. To most effectively secure customer data and thereby protect consumer privacy, all entities that store or process sensitive personal information, and all entities with access to customer financial information, should be subject to and maintain well-recognized standards such those in the Gramm-Leach-Bliley Act and implementing regulations.

Below is a general overview of some of the legal and regulatory requirements to which banks are subject, and for which they are examined and supervised. These requirements include, but are not limited to, the Gramm-Leach-Bliley Act, the “Interagency Guidelines Establishing Information Security,” and the Federal Financial Institutions Examination Council’s IT

Examination Handbook. The measures outlined below demonstrate how banks safeguard customer PII. To fully protect citizens, all entities should be required to safeguard PII in a comparable manner.

I. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (“GLBA”) and its implementing regulations require financial institutions to disclose their information-sharing practices to their customers and to safeguard sensitive data. Additionally, Section 501(b) of the GLBA requires federal banking agencies to establish standards for protecting the security and confidentiality of financial institution customers’ non-public personal information.

Subtitle B of GLBA prohibits any person from receiving customer information about another person whether by making a false, fictitious or fraudulent statement to a financial institution representative, to a customer of a financial institution or providing any fraudulent document to a financial institution.⁵

See <https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf> and <https://www.occ.treas.gov/newsissuances/bulletins/2000/bulletin-2000-21a.html>

⁵ 15 U.S.C. 682i

II.² Interagency Guidelines Establishing Information Security

The banking agencies issued their “Interagency Guidelines Establishing Information Security” (“Guidelines”)⁶ to implement the GLBA requirements. Generally, the Guidelines establish administrative, technical and physical safeguard standards to ensure the security, confidentiality, integrity and proper disposal of customer information.

The Guidelines apply to customer information maintained by, or on behalf of, financial institutions. The Guidelines, among other requirements, mandate that financial institutions implement “a written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the bank and nature and scope of its activities.”³

The Guidelines also specify that the board of directors or an appropriate committee of the board of each insured depository institution shall be involved in approving and overseeing the written information security program.

² C.F.R. Part 30, Appendix B.

³ Federal Register. Vol 66. No. 22. Page 8619.

Each institution is required to assess risk by identifying reasonably foreseeable internal and external threats, and the likelihood and potential damage of those threats. Each institution must also assess the sufficiency of policies, procedures, customer information systems and other arrangements in place to control risks. There are also extensive requirements for managing and controlling the risk which include implementation of a response program.

Finally, it is important to point out that entities contracted by financial institutions are also required to protect customer information in the same manner as the financial institution.^{4,5}

III. *Federal Financial Institutions Examination Council ("FFIEC") IT Examination Handbook*⁶

Other legal and regulatory guidance also adequately dictate bank privacy procedures. For example, the Federal Financial Institutions Examination Council's IT Examination Handbook ("FFIEC IT Handbook") is an authoritative document which outlines various guidelines concerning customer data security and privacy that are rightly intertwined within all operational aspects of the bank – from governance to third-party management to information technology.

Breach Notification

ICBA continues to support a single national breach notification standard. Similarly, any legislation related to privacy or data security should also preempt state laws to prevent a continuing patchwork approach to these policy areas.

If a bank becomes aware, upon an investigation, that customer information was improperly accessed, it must notify the affected customers with a description of the incident and what customers may do to protect themselves. This is not true for all entities that store and process sensitive personal information, although it has become a matter of good business practice to notify impacted customers.

Regarding customer notification, ICBA submitted a statement for the record last year for a hearing entitled "Data Security Legislative Solutions: The Community Bank Perspective," which was held before the U.S. House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit on March 7, 2018. Prior to the hearing, then Subcommittee

⁴ Board of Governors of the Federal Reserve System. Interagency Guidelines Establishing Information Security Standards "Small Entity Compliance Guide". 2.

⁵ To enhance the protection of privacy, ICBA also suggests, in response to Question 3, examination and supervision of all third parties.

⁶ See: <https://ithandbook.ffiec.gov/>

Chairman Blaine Luetkemeyer and Representative Carolyn Maloney circulated a discussion draft of a data security bill, the “Data Acquisition and Technology Accountability Act.”⁷

That discussion draft would have created a national data breach notification standard to replace the current patchwork of differing state breach notification laws. In an integrated national economy with a geographically mobile population, consistent standards and expectations are needed to avoid consumer confusion.

Our statement conveyed support for the security requirements in the discussion draft, which would subject other entities to a scalable data security standard. Community banks have long been subject to regulatory mandates that set rigorous data protection practices. These mandates are fundamental and a critical component of the safety and soundness of the overall banking system. With data breaches in the news almost daily, the status quo advocated by other sectors is simply not working for American consumers. Consumers demand that their personal information be held securely and not subject to innumerable breaches. The only way to fulfill this demand is by raising the bar to ensure all entities are subject to comparable standards.

Question 2: What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?

ICBA supports the current privacy notice requirements. Banks are currently required, through law and regulation, to provide privacy notices and a myriad of disclosures to consumers and customers about the information they collect and share and the purpose of the information.

Disclosure

ICBA supports the current privacy notice requirements. Under current law and regulation, banks must provide privacy disclosures to consumers and customers. Privacy notices must describe whether and how the financial institution shares consumers’ nonpublic personal information with other entities.¹² The notices must also briefly describe how financial institutions protect the nonpublic personal information they collect and maintain.¹³

⁷ For bill text, see: <https://republicans-financialservices.house.gov/uploadedfiles/bills-115-datasa-pih.pdf>

An initial notice must be provided when a customer relationship is established.¹⁴ An annual notice must be sent to consumers if the institution has changed its privacy policy since disclosure of its most recently sent privacy policy and if financial institution limits their sharing of customer information.¹⁵ If an institution chooses to disclose nonpublic personal information about a consumer to a nonaffiliated third party, the institution is required to deliver an annual privacy notice.¹⁶ GLBA Section 502 and Regulation P also require that the disclosures provide information for the consumer to opt-out of sharing of personal information with certain nonaffiliated third parties with some exceptions.¹⁷

¹² 12 CFR 1016.6(a)(1)-(5), (9)

¹³ 12 CFR 1016.6(a)(8)

¹⁴ 12 CFR 1016.4(a)(1), 1016.5(a)(1). Financial institutions are also required to provide initial notices to consumers before disclosing any nonpublic personal information to a nonaffiliated third party outside of certain exceptions.¹⁵ A financial institution that does not share nonpublic personal information with nonaffiliated third parties, unless required to do so under certain exceptions, is not required to provide an annual notice. These exceptions include, for example, providing information to third party service providers, securitization, law enforcement and compliance, and consumer reporting; and certain other disclosures described in the GLBA and Regulation P as exceptions to the opt-out requirements. See Bureau of Consumer Financial Protection, 12 CFR 1016, "Amendment to the Annual

Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P)" Final Rule. Published 9 August 2018. https://files.consumerfinance.gov/f/documents/bcfrp_glba-privacy-notices_final-rule_amendment_201808.pdf.

¹⁶ 12 CFR 1016.4(a)(1), 1016.5(a)(1). Financial institutions are also required to provide initial notices to consumers before disclosing any nonpublic personal information to a nonaffiliated third party outside of certain exceptions.

¹⁷ See Bureau of Consumer Financial Protection, 12 CFR 1016, "Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P)" Final Rule. Published 9 August 2018. Page 6. See also 15 U.S.C. 6802(a), (b)(2), and (e); 12 CFR 1016.13, 1016.14, 1016.15.

Information Collection, Regulatory Compliance and Disclosure

In addition to collecting the customer information necessary to provide financial services, financial institutions are required, by statute or regulation, to collect information about consumers and customers in the normal course of doing business to meet regulatory requirements, including obligations to detect and disrupt illicit financial activity. Oftentimes, banks will rely on access to information available from third parties to gather information about customers, particularly in compliance with anti-money laundering "Know Your Customer" rules and Office of Foreign Asset Control obligations. A sampling of these regulatory collection and disclosure laws are detailed below.

The Nation's Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org

I. Bank Secrecy Act

The Bank Secrecy Act and its implementing regulations¹⁸ require the collection and storage of personal information. As part of an effective customer due diligence program a bank must collect and verify the identifying information from each customer before opening the account, including a customer's name, date of birth, address and identification number. At a minimum, a bank must retain this data for a period of five years after an account is closed. The bank must also keep a description of any document that was relied on to verify identity, such as an unexpired driver's license, for five years. Furthermore, a bank should have a thorough understanding of the money laundering or terrorist financing risks of its customer base by collecting information sufficient to develop an understanding of normal and expected activity for its customers. This includes collecting additional data for various transactions, such as wire transfers, the purchase and sale of monetary instruments, and funds transfers.

II. Electronic Fund Transfer Act

The Electronic Fund Transfer Act ("EFTA") requires a disclosure to consumers when using electronic funds transfer ("EFT") that, in the ordinary course of doing business, the financial institution may provide information concerning the consumer's account to third parties (Section 205.7(b)(9)). A financial institution must describe the circumstances under which any information, relating to an account to or from which EFTs are permitted, will be made available to third parties.¹⁹

III. Right to Financial Privacy Act

On certain occasions, government authorities may request a customer's financial records. The Right to Financial Privacy Act ("RFP") establishes guidelines that government authorities must follow when requesting a customer's financial records. The RFP also outlines specific procedures the financial institution must follow upon receiving such a request. This includes,

¹⁸ Federal Register. Vol. 81, No. 91. 11 May 2016. <https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/201610567.pdf>. 29398.

¹⁹ 12 CFR 1005.
among other provisions, providing a customer notice before the financial institution discloses the customer's financial records.²⁰

IV. Home Mortgage Disclosure Act

The Nation's Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org

The Home Mortgage Disclosure Act (“HMDA”), implemented by Regulation C, requires many financial institutions to collect, maintain, report, and publicly disclose loan-level information about mortgages. HMDA’s original purpose was to provide the public and public officials with data to help determine whether financial institutions are serving the housing needs of the communities in which they are located, and to assist public officials in their determination of the distribution of public sector investments in a manner designed to improve the private investment environment. Congress later expanded HMDA to require financial institutions to report racial characteristics, gender, and income information on applicants and borrowers. On an annual basis, HMDA requires that its loan/application register (“LAR”) data be submitted and that the institution retain a copy of its LAR for at least three years.

V. The Dodd-Frank Wall Street Reform and Consumer Protection Act

Section 1100F of The Dodd Frank Wall Street Reform and Consumer Protection Act (the “Dodd Frank Act”) requires a disclosure to the consumer if a credit score was used in taking adverse action on a credit application. Section 615(a) of the Fair Credit Reporting Act (“FCRA”), as amended by the Dodd-Frank Act, requires a person to provide an adverse action notice when the person takes an adverse action based in whole or in part on information in a consumer report. The FCRA’s requirements for adverse action notices apply only to consumer transactions and are designed to alert consumers that negative information was the basis for the adverse action. A creditor that obtains a credit score and takes adverse action is required to disclose that score, unless the credit score played no role in the adverse action determination. Adverse action notices typically adopt the format of the model form provided by the Consumer Financial Protection Bureau (“CFPB”) and should disclose that adverse actions were taken based on information provided from a consumer reporting agency and that the consumer has the right to dispute the accuracy or completeness of any information in a consumer report, among other provisions.

²⁰ 12 U.S.C. 3401, *et seq.*

Question 3: What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?

The Nation's Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org

Banks are required to collect certain PII based on various regulatory requirements and provide that information to prudential regulators. Prudential regulators must also appropriately safeguard that information. Additionally, as an added consumer protection, third parties that contract with banks for services which are not currently subject to examination and supervision should also be examined and supervised for their compliance with the Interagency Guidelines Establishing Standards for Safeguarding Custom Information (“Guidelines”), implementing GLBA.

Prudential regulators must also appropriately safeguard consumer information

As illustrated in the previous answer, there are numerous regulatory requirements by which banks must collect PII and then share that information with financial regulators. It is critical that the prudential regulators maintain the confidentiality of the information provided to them.

No company, financial institution, or government agency is exempt from insider threats or criminals breaking into their systems and yanking the personal information of their customers, employees, and/or general stakeholders. In fact, the prudential banking regulators have had their share of data security incidents. For example, in November 2015, a former employee at the Office of the Comptroller of the Currency removed more than 10,000 records by downloading files onto thumb drives without receiving prior authorization.⁸ In 2018, the Federal Deposit Insurance Corporation’s Office of Inspector General released a “Special Inquiry Report,” which detailed several data incidents and a data breaches, one in which an employee placed data on personal storage devices.⁹ The Federal Reserve appears to have been under constant attack by would-be hackers according to news reports in mid-2016; whether hackers have been successful in accessing sensitive records remains to be seen.¹⁰ In 2014, a National Credit Union Administration examiner lost a flash drive containing personal information for members of a credit union in Palm Springs, California.²⁴ Additionally, the CFPB paused the collection of personally sensitive data from companies until an independent review found that “externally facing bureau systems appear to be well-secured.”¹¹

⁸ OCC. “OCC Notifies Congress of Incident Involving Unauthorized Removal of Information.” 28 October 2016. <https://www.occ.gov/news-issuances/news-releases/2016/nr-occ-2016-138.html>

⁹ FDIC, Office of Inspector General. “Special Inquiry Report: The FDIC’s Response, Reporting and Interaction with Congress Concerning Information Security Incidents and Breaches. April 2018. OIG 18-001. <https://www.fdicig.gov/sites/default/files/report-release/OIG-18-001.pdf>

¹⁰ Reuters. “Exclusive: Fed Records Show Dozens of Cybersecurity Breaches.” 2016. June

1. <https://www.reuters.com/article/us-usa-fed-cyber-idUSKCN0YN4AM> ²⁴ Credit Union Times. “NCUA Examiner Blamed for Data Breach. 15 December 2014.

<https://www.cutimes.com/2014/12/15/ncua-examiner-blamed-for-data-breach/>

¹¹ Wall Street Journal. “CFPB to Resume Private Consumer Data Collection. 31 May 2018. <https://www.wsj.com/articles/cfpb-to-resume-private-consumer-data-collection-1527796179>

The Nation's Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org

ICBA is troubled that liability from a potential breach into any of the prudential regulators' systems could be unfairly assigned to community banks that securely submitted their data. Too often, the breached entity skates by while financial institutions are left to mitigate damages to their customers. For example, when Home Depot was breached in 2014, community banks were responsible for replacing payment cards, notifying customers, implementing enhanced monitoring, and reimbursing customers for fraudulent transactions. In the recent Equifax breach, sensitive personal information was accessed by a yet-unknown source. Community banks will face untold damages due to the unique circumstances of this massive data breach. Because of the Equifax breach, community banks must institute additional protective measures to deter customer identity theft and fraudulent transactions. Community banks will also bear the responsibility for costs associated with payment card cancellation and replacement, fraudulent charges, customer notification, closing affected accounts, and lost interchange fees; all while monitoring the risk of continuing to exchange information with Equifax. A breach into the prudential regulators' systems could have strikingly similar effects on the nation's community banks, particularly when considered in context of the data incidents described above.

Third Party Examination and Supervision

The protection of personal information is critical to protecting customer privacy. Banks contract with third parties for a variety of reasons, some of which include adding efficiency to back office operations. At times, it becomes necessary to share sensitive personal information with third parties. According to the FFIEC IT Handbook, banks that have contractual relationships with third parties and share personal information with these third parties are required to oversee service provider arrangements by (1) exercising appropriate due diligence in selecting service providers; (2) requiring service providers by contract to implement appropriate measures designed to ensure the security and confidentiality of the institution's "customer information"; and (3) where indicated by the institution's risk assessment, monitoring service providers to confirm that the service providers have satisfied their contractual obligations, including by reviewing audits, summaries of test results, or other equivalent evaluations of service providers.

²⁶

As an added protection for consumers, examinations of all third parties would ensure that third parties are safeguarding consumer data in compliance with GLBA and will ultimately better protect the consumer.

²⁶ See the FFIEC IT Examination Handbook on Information Security, Sections II and III.D. Also see the

Outsourcing Technology Services Booklet – “Before entering into outsourcing contracts, and throughout the life of the relationship, institutions should ensure the service provider’s physical and data security standards meet or exceed standards required by the institution. Institutions should also implement adequate protections to ensure service providers and vendors are only given access to the information and systems that they need to perform their function. Management should restrict their access to financial institution systems, and appropriate access controls and monitoring should be in place between service provider’s systems and the institution.”

Question 4: What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?

ICBA recommends that the credit reporting agencies (“CRAs”), also known as credit bureaus, be subject to comparable supervision and examination as banks. Additionally, CRAs should focus on educating and informing the consumer about the use of credit reports and their consumer data collection and sharing practices.

Protecting Consumer Data

Protecting consumer data is a critical component to maintaining the financial services ecosystem. Banks are held to a high standard as explained in the previous responses. However, CRAs are not subject to the same supervision and examination as banks, despite the vast amount of PII they process, maintain and store. For example, the credit bureaus must comply with rules set by the Federal Trade Commission and CFPB with regard to selling consumer data, but they are not subject to the same examination and supervision as banks.

Last Congress, Representative Patrick McHenry introduced H.R. 4028, which, among other things, would subject CRAs to examination and supervision by a banking regulator to be determined by the FFIEC. ICBA strongly supported, and continues to support, this approach.

The massive data breach at Equifax, which exposed the personal data of 148 million American consumers, shows the ongoing vulnerability of CRAs. While CRAs are subject to the data security standards of the Gramm-Leach-Bliley Act (GLBA), they are not examined or supervised for their compliance with these standards in the same manner as financial institutions, yet they hold equally critical, personally sensitive information about consumers. This is a grave weakness and disparity in our current system.

Data Accuracy

Accurate information within a credit file is critical for end-users of credit reports. These reports are used to make important decisions about a customer’s ability to obtain and responsibly use credit. CRAs should educate and inform consumers about the use of credit reports and their

The Nation’s Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org

information collection and sharing practices. Education should stress to the consumer the importance of ensuring their reports contain accurate, complete and verifiable information, and the steps taken to secure data.

Question 5: What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

Non-bank entities accessing customer account data must be held responsible for ensuring the safety and security of the consumer information they are accessing and must be held liable for any data breaches and consumer harm which they cause. At a minimum, consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.

While ICBA fully supports consumers' rights to have access to their own information, such access should be properly balanced with ensuring that consumer privacy is not needlessly threatened. Protecting the privacy of consumer information is at the heart of the community bank business model. Community banks are strong guardians of the security and confidentiality of customer information as a matter of good business practice.

Information that is gathered by entities outside of the financial services industry is not held to the same standard as it relates to safeguarding information. Once information is shared with permissioned third-parties, consumers may no longer have control of their personal and financial information. The potential for abuse is real and can be extremely harmful to consumers. This leaves consumers vulnerable to entities that may mislead them about who they are or what they do with the information they collect and places an extraordinary burden on consumers to be vigilant in their research and knowledge of firms to which they may provide their online account credentials. For this reason, ICBA has profound concerns that non-bank entities which may be authorized by consumers to access their information and store their bank login credentials do not take the same care in protecting consumer privacy and data as community banks. It is also worrisome that many third parties which seek to access customer data are not well capitalized and may have no real assets. In fact, these firms may be no more than one person developing an app on his or her laptop. When there is a loss, they may be financially unable to make the consumer whole.

The Nation's Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org

While financial institutions are prohibited from sharing account numbers or similar access codes for marketing purposes, and from sharing personal information with nonaffiliated third parties without giving customers an "opt-out notice" that describes customer's rights to information being shared, other non-financial entities are not subject to the same rules. Selling consumer data for marketing purposes is an appealing revenue source which could be utilized by some unscrupulous businesses.

At a minimum, consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.

To further privacy protections, there is opportunity to set limits and safeguards on which data is available to data aggregators, data brokers and other third-parties. Granting carte blanche access to these entities increases the potential for unauthorized use and inadvertent breaches. In addition to setting limits on the type of data collected, Congress has an opportunity to limit how thirdparties and data aggregators use the data. These limitations should reflect the reasonable expectations of consumers or explicit consumer instructions on the use of such data.

Data aggregators and other third-parties should also provide transparency on data access. If data aggregators and third-parties seek permission from consumers to access a their data, then consumers should be provided with clear disclosures on which data is being collected and how it will be used, along with any downstream usage of that data, (i.e., if and whether it will be soldoff to any subsequent third-parties).

Finally, to ensure that any legislation, regulation, or best practices is implemented by data aggregators and other third-parties, the CFPB should have formal and explicit supervision and enforcement authority over these entities.

While data aggregators and other third-parties are focused on accessing and utilizing consumer data, there must be a serious recognition that not all data is equal. Financial data is unlike all other forms of data, and as such, must be accessed and used with the utmost caution. As Congress continues to examine and explore this area, it is incumbent for legislation, regulation, or best practices to address these issues.

Community Banks Should Not Have to Bear the Cost and Risk of Ensuring Safe Third-Party Access

The Nation's Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org

As community-based institutions, a community bank's success is in large part dependent on its reputation. Maintaining the integrity of customer accounts is of utmost importance to community banks, not only because it is required by law, but also because it is the right thing to do. If a customer experiences an adverse event which results in financial loss caused by a breach or failure by a permissioned third party, it is likely that customer will look to his or her bank with the expectation of being made whole. When a loss occurs through no fault of a community bank, but because of the failing of a third party, that third party should be held responsible. For example, there should be certainty as to whether consumers would be protected under the Electronic Fund Transfer Act for unauthorized debits when consumers share their account information.

Furthermore, community banks have a vital stake in containing any damage caused by hackers, identity thieves and breaches to third parties. Regardless of where a breach occurs, banks are the stewards of the customer financial relationship. They take measures to restore consumer confidence in the financial system and absorb any upfront costs, which may be significant, of third-party intrusions by responding to customer concerns and inquiries, protecting against fraud and absorbing other expenses. Therefore, any costs associated with a breach or hack should be borne by the entity that incurs the breach. Firms with third-party access to a consumer's account should bear full liability for any consumer harm resulting from a breach to its system.

ICBA appreciates the opportunity to provide our views on these questions. We welcome a further discussion with the Committee on these and other related topics. Should you have any questions, please reach out to Jeremy Dalpiaz of my staff by email at Jeremy.Dalpiaz@icba.org or by phone, 800-422-8439.

Sincerely,

Rebeca Romero Rainey
President and CEO

The Nation's Voice for Community Banks.®

WASHINGTON, DC	SAUK CENTRE, MN	
1615 L Street NW	518 Lincoln Road	
Suite 900	PO Box 267	866-843-4222
Washington, DC 20036	Sauk Centre, MN 56378	www.icba.org