S. HRG. 116–182

DATA OWNERSHIP: EXPLORING IMPLICATIONS FOR DATA PRIVACY RIGHTS AND DATA VALUATION

HEARING

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ON

EXAMINING THE CONCEPT OF PERSONAL DATA OWNERSHIP, INCLUDING ITS EFFICACY ON ENHANCING INDIVIDUALS' PRIVACY AND CONTROL OVER THEIR PERSONAL INFORMATION

OCTOBER 24, 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

40–382 PDF WASHINGTON : 2021

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*

BRANDON BEALL, *Professional Staff Member*
ALEXANDRA HALL, *Professional Staff Member*

JAN SINGELMANN, *Democratic 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

THURSDAY, OCTOBER 24, 2019

WITNESSES

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

DATA OWNERSHIP: EXPLORING IMPLICATIONS FOR DATA PRIVACY RIGHTS AND DATA VALUATION

THURSDAY, OCTOBER 24, 2019

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

The Committee met at 10 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 Committee will come to order.

We would like to welcome today to the Committee four witnesses with extensive experience and a range of perspectives on issues related to data ownership, valuation, and privacy, including Mr. Jeffrey Ritter, Founding Chair of the American Bar Association Committee on Cyberspace Law and an external lecturer at the University of Oxford—and I guess you are on research sabbatical—Mr. Chad Marlow, Senior Advocacy and Policy Council at the American Civil Liberties Union; Mr. Will Rinehart, Director of Technology and Innovation Policy at the American Action Forum; and Ms. Michelle Dennedy, Chief Executive Officer of DrumWave.

As a result of an increasingly digital economy, more personal information is available to companies than ever before. Private companies are collecting, processing, analyzing, and sharing considerable data on individuals for all kinds of purposes.

There have been many questions about what personal data is being collected, how it is being collected, with whom it is being shared, and how it is being used, including in ways that affect individuals' financial lives. Given the vast amount of personal information flowing through the economy, individuals need real control over it.

This Committee has held a series of data privacy hearings exploring possible frameworks for facilitating privacy rights to consumers. Nearly all have included references to data as a new currency or commodity.

The next question, then, is, who owns it? There has been much debate about the concept of data ownership, the monetary value of personal information, and its potential role in data privacy. Some have argued that privacy and control over information could benefit from applying an explicit property right to personal data, similar to owning a home or protecting intellectual property. Others

contend that the very nature of data is different from that of other tangible assets or goods.

Still, it is difficult to ignore the concept of data ownership that appears in existing data privacy frameworks. For example, the European Union's General Data Protection Regulation, or GDPR, grants an individual the right to request and access personally identifiable information that has been collected about them.

There is an inherent element of ownership in each of these rights, and it is necessary to address some of the difficulties of ownership when certain rights are exercised, such as whether information could pertain to more than one individual or if individual ownership applies in the concept of derived data.

Associated with concepts about data ownership or control is the value of personal data being used in the marketplace and the opportunities for individuals to benefit from its use.

Senators Kennedy and Warner have both led on these issues, with Senator Kennedy introducing legislation that would grant an explicit property right over personal data and Senator Warner introducing legislation that would give consumers more information about the value of their personal data and how it is being used in the economy.

As the Banking Committee continues exploring ways to give individuals real control over their data, it is important to learn more about what relationship exists between the true data ownership and individual's degree of control over their personal information; how a property right would work for different types of personal information; how data ownership interacts with existing privacy laws, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the GDPR; and different ways that companies use personal data, how personal data could be reliably valued and what that means for privacy.

I appreciate our witnesses today for offering their expertise and sharing their unique range of perspectives on these issues.

Senator Brown.

OPENING STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thank you, Mr. Chairman, for calling this hearing.

Welcome to all four witnesses. A special welcome to Jeffrey Ritter, whom, shall we say, we knew each other 40 years ago. I will leave it at that. At the Statehouse in Columbus.

This Committee has spent some time over the last several months discussing Facebook's poorly—no other adverb to describe it—poorly thought-out plan to create a global currency. The bottom line is we know that Facebook simply cannot be trusted with Americans' personal information. It is terrible at protecting its users' privacy. It was pretty clear the last thing we should do is trust them with America's currency.

It is not just Facebook. Every time corporations in Silicon Valley come up with a new business model, the result is the same. They get more access to our personal data, spending habits, location, the websites we visit, and it means more money in their pockets. Everyone else gets hurt.

So I want to begin this hearing with a simple question. Who has the right to control your personal, private information? You or Silicon Valley CEOs like Mark Zuckerberg?

I think we all agree that Americans should have more control over their private information, but should we treat that private information just like property? Today's witnesses will discuss that idea.

At first glance, it might seem like a simple way to tackle the common problems, the complex problems created by data collection and machine learning. The promise is that if we just treat personal data like property, markets will do the hard work of protecting our privacy for us. We all know that is not how it will work.

Instead of making companies responsible for protecting their customers' privacy, this idea puts the burden on all of us individually and collectively.

Now imagine if every time you wanted to use Facebook or pay for something with an app or login to a Wi-Fi network, you had to read even more legal fine print and then check a box saying, "OK, I waive my personal right to my data to use this service," or you had to join some kind of data collective to sell your data.

Working people in this Country have enough to worry about: trying to get the kids out the door in the morning, get to work on time, make rent, save for college, pay the bills. The idea that people should also have to manage their data like a landlord manages its tenants is just ludicrous.

It should be pretty simple. Corporations should not be allowed to invade our privacy. We know that today they are.

But think about all the personal data that is already floating around out there. Equifax exposed the personal information of more than 150 million Americans: Social Security numbers, birthdays, addresses. Capital One exposed the personal information of more than 100 million Americans. How can you own your data when it is already littered all over the internet?

Big tech companies does not want to protect your personal information. They want to profit off it. Protecting your privacy does not make them any money. It costs them money. So they are simply not going to do it.

They want your data. They want to get it for free. They want to pay as little as possible if they cannot get it for free.

So it should be no surprise that I am skeptical—I think most of us up here are quite skeptical—when I hear of plans for America's data to be treated, again, like property.

If Americans want more control over their private information, we have to find a way to prevent corporations from mining our data and selling it to each other. Creating a supermarket for selling away our privacy does the opposite. Treating data as something that can be owned and bought and sold does not solve any of these problems, especially when undermining our privacy is the business model.

Mark Zuckerberg and his Silicon Valley buddies want us to skip over the part when we have control over our own privacy, and they want to jump to the part where giant tech companies get to use their market power to squeeze our privacy out of us, and it would all be legal. That is not acceptable.

I appreciate that Chairman Crapo has been working with me in a bipartisan way. There is a lot of interest in this Committee in doing it right to create real privacy protections. Privacy is not partisan. It is a basic right.

I look forward to continuing our work together, Mike.

Chairman CRAPO. Thank you.

We will now proceed to the testimony. I have already introduced each of our witnesses, and we will proceed in the order that I introduced you. I ask you to please pay attention to the 5-minute rule, and I ask the same thing of our colleagues here.

Mr. Ritter, please proceed.

STATEMENT OF JEFFREY RITTER, FOUNDING CHAIR, AMERICAN BAR ASSOCIATION COMMITTEE ON CYBERSPACE LAW, AND EXTERNAL LECTURER, UNIVERSITY OF OXFORD, DEPARTMENT OF COMPUTER SCIENCE (ON RESEARCH SABBATICAL)

Mr. RITTER. Thank you. Good morning, Chairman Crapo, Ranking Member Brown, and Members of the Committee.

I join you today to speak in the role as an active contributor for over 30 years to law reforms enabling the United States and global electronic commerce, privacy, and information security.

Speaking bluntly, the time is long overdue for this hearing and the work of this Senate Committee and the Senate and the Congress to develop comprehensive privacy reform. Right now, we have basically been relegated to playing catch-up with the Europeans and other nations that are embracing the rules they have written. We are trying to weave together what we have into some type of whole cloth that is new.

But privacy law reform will surely fail if we do not address the issues that have been focused on by the Chair and by Senator Brown in their opening remarks. There is a fundamental question. It does need to be answered. Who owns digital information? It is not any question that it is an asset of human society in the 21st century, but is it something that can be owned?

In the totality of all digital information, we have, in Senator Brown's words, skipped over it. For billions and trillions of dollars of development over the last 30 years, no one has given an answer.

For personal information, this question is even more important. Yes, it is identifiable, but who truly owns it? Who can control it?

From a perspective of decades working in the international scene, trying to advance these rules, I would observe that the United States once led the world writing the rules for electronic contracting, electronic signatures, and electronic commerce to work, but at this point, we are falling behind.

So I would suggest that we need to do something new. We need to reestablish this Nation's leadership by confronting this very hard question and incorporating it into our privacy reforms. Clear, explicit rules are needed.

I may disagree with Senator Brown's opening remarks about figuring out that it should be owned or not owned as property by whom, but we needed to clarify these rules so that we can, in fact, control the uses and misuses of this information.

It is only by crafting those rules that we can then enhance and enable acquiring, using, transferring, selling, sharing, controlling data. We have got to know whose it is so we can make someone accountable.

Every commercial system built on the rule of law for real estate, banking, consumer products, industrial products begins with a commitment to define and protect the owner of the property. Yet across the digital world we now live in, particularly for privacy and individual data, while the data subject has controls, the fundamental question has not been answered. Who owns it?

This is not a question that is being addressed in isolation here in the United States. As summarized in an article that I included in our written testimony, German, Japan, and the OECD are all calling for formal legal rules on ownership, including Chancellor Merkel herself. Japan has already published model guidelines for structuring data sharing and licensing agreements based on ownership principles, not yet translated in English, allowing Japanese companies to build commercial momentum in being able to engage in these kind of transactions.

So I submit, humbly, that failing to address data ownership in our privacy reforms will further isolate the United States and allow the rules for data and data as property to be written by others.

Now, the solutions for crafting this legal concept are already part of Federal law. They were incorporated into the laws governing electronic transferable records and in U.N. model laws that have recently been approved with substantial U.S. input and influence.

There, the rights of ownership are exercised by establishing and maintaining control of the file. Now, under this principle, realistically, the first owner of the information will be the business entity with whom the data subject is engaging—the bank, the hospital, the university. After all, they are the ones that have the systems that establish the control over the information.

But I do believe that recognizing ownership should not do anything to diminish or remove a data subject's controls. We cannot keep the world's systems from engaging with our information, but we can regulate it and recognizing the property rights are more clear. It is going to help the process.

So, in closing, just let me begin by emphasizing the opportunity, not the obstacle. Clarifying these rules, reconciling controls with ownership, will not only improve a data subject's—individual's control of their information but will, in fact, foster greater accountability for the misuse of that information against the individual's interest.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you very much.

Mr. Marlow.

STATEMENT OF CHAD A. MARLOW, SENIOR ADVOCACY AND POLICY COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Mr. MARLOW. Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for the privilege of testifying before you today.

I serve as a Senior Advocacy and Policy Counsel at the ACLU, where my principal focus is on issues involving privacy and

technology. In that role, I spend a great deal of time with the ACLU's 53 affiliates throughout the Nation learning about and taking positions on State-level privacy legislation.

Over the past year, I have encountered numerous State efforts to enact data-as-property laws, and today I would like to share what I have learned.

In the 2019 State legislative sessions, data's property laws were pursued or introduced in 11 States. To illustrate those States' experiences, I am going to focus on the effort in the State of Oregon.

In Oregon, where the bill specifically sought to treat personal health information as property, the leading talking point of the bill was that it was pro-privacy. Such a law, the argument went, would give people the right to authorize the sale of their data and to receive a portion of the proceeds in return. It is notable that what that amount might be was never actually discussed.

The pro-privacy part of the pitch was that persons could also elect to not have their data sold. The presentation proved persuasive. Forty lawmakers out of 100 in the entire legislature signed on to sponsor the bill at the time it was introduced.

But then something happened. Legislators started to learn more about what the data's property model looks like when it is put into practice, and they became concerned that the model was not pro-privacy after all.

The basis for these concerns was threefold. First, in order to effectuate the data-as-property model, at the same time a patient's personal information was collected and they were notified of their privacy rights, the power of the Government would be applied to essentially advertise the option to forego those rights by selling away one's personal information. Lawmakers grew uncomfortable with the sense they were facilitating this anti-privacy choice.

Second, lawmakers became concerned about adopting a model where persons with less wealth were likely to end up with less privacy. They recognized that Americans who were economically secure would find it easy to reject offers to sell their private information, but they also knew that might not be the case for an elderly person who has a hard time affording their prescriptions and rent or that it might be too tempting a sales pitch for a family that is struggling to put food on their table.

Lawmakers also started to appreciate how a Government-endorsed data-as-property law might serve to further expand the existing digital divide, where persons enduring socioeconomic and regional economic disadvantages, including disproportionately persons of color, already have less privacy because they are forced to rely on more affordable but less privacy protective technology products and services.

Third, lawmakers were concerned that enacting a data-as-property model would require the application of a unique tracking identifier to all personal information, which they were especially weary of, given the model's ability to expand beyond the healthcare context. Privacy and the ability to remain anonymous might both be casualties of the effort to turn data into property.

In the end, Oregon State legislature, despite 40 percent of its members having originally sponsored the bill, wisely abandoned the data's property model, and the bill died. Ultimately, lawmakers

in all 11 States in which the data's property bill was pursued came to the same conclusion, and not a single bill passed.

In the laboratories of democracy, the data-as-property experiment is failing to gain traction, but let me end my testimony on a positive note from our State legislatures.

In 2019, two State laws were adopted that made important advances in protecting privacy without treating data as property. The California Consumer Privacy Act, which among its many achievements allows consumers to opt out of their personal information being sold, and Maine's Act to protect the privacy of online customer information, which takes the superior approach of not allowing a person's information to be sold without first securing their opt-in permission, these efforts should be studied, replicated, perhaps improved upon, and most of all respected by Congress by not preempting the privacy protections that they have achieved.

The high value Americans place on their privacy is universal, nonpartisan, and wisely enshrined in our Bill of Rights. The proper response to the pervasive loss of individual privacy is to pass stronger privacy laws, not just to throw up our hands and conclude the only issue left to tackle is who gets the money.

Congress has the ability to adopt strong privacy laws without relying on models that undermine privacy in the process, and I have every confidence that you will.

Thank you again for the opportunity to testify today.

Chairman CRAPO. Thank you.

Mr. Rinehart.

STATEMENT OF WILL RINEHART, DIRECTOR OF TECHNOLOGY AND INNOVATION POLICY, AMERICAN ACTION FORUM

Mr. RINEHART. Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you again for the opportunity to testify before you today on the issue of data property rights.

Like others in privacy, I am skeptical that a data property right is actually the best policy mechanism for ensuring privacy. My written testimony today actually goes into far more detail, but I want to highlight three important points that I feel are necessary to point out.

First all, a privacy—a property right to personal data is not necessary to, in fact, secure privacy, and in fact, it could be an efficient one economically.

Second, valuing data is often difficult because raw or personal data is not what is in demand but, in fact, the insights that are built on top of it.

And, third, regardless of the privacy regime that is adopted, privacy laws will create an unavoidable cost from compliance, which will reverberate throughout the economy.

Data ownership seems to fit naturally with our common experience in relationship with technology, but I think there are fundamental reasons to be skeptical. Since my fellow panelists focused on some of the legal side of things, I want to highlight one area that concerns me.

It is really unclear if the assignment of data property rights will actually align all of the incentives between users and firms. In particular, if a broad right to data is established, users would be

forced to search for innovative opportunities. While some see this as a plus, I think, in reality, it would actually be a burden. Assigning property rights in data will dramatically change who can say no to any potential innovation. Users would be forced to become their own data entrepreneurs.

In this world, users would become—rather, users would learn what companies already know, which brings me to my second point.

Valuing personal data is often very difficult because what is in demand are actually the insights that are built on top of that data. In my written testimony, I go into far more detail and, in fact, lay out the four basic methods to price data, but the takeaway, I think, is pretty abundantly clear. There is no perfect way to value data, and it is highly context-dependent.

I think one story really highlights this tension. So when Caesars Entertainment went bankrupt a couple years back, the Total Rewards customer program got valued at nearly $1 billion, which made it the most valuable asset in the proceeding. Even though it was not sold off, the ombudsman privacy report understood that it would actually be a very tough sell because of the difficulties incorporating it into another customer loyalty program.

The Total Rewards example, I think, underscores a pretty, particularly important characteristic of data. It is often valued within a relationship or a firm relationship, but it is often difficult to value outside of that firm relationship.

For my third and final point, I really want to highlight what I think is probably the most important thing to note here, that regardless of the particular policy mechanism that is chosen for privacy, these laws will create unavoidable costs from compliance, which will impact investment opportunities in countless industries.

We have already seen this in Europe where investment from venture capital had gone down at least in the short term by some 39 percent.

In the United States, California's CCPA was estimated by its own State agencies to cost nearly 1.8 percent of gross State product, which is quite massive.

And the ITIF, a think tank here in the DC area, estimated that a Federal privacy law could cost as much as $122 billion per year. All this reminds me of one of my favorite authors, Seth Godin, who once remarked, "The art of good decisionmaking is looking forward to and celebrating the tradeoffs, not pretending that they do not exist."

I thank you for your time, and I look forward to questions.

Chairman CRAPO. Thank you.

Ms. Dennedy.

STATEMENT OF MICHELLE DENNEDY, CHIEF EXECUTIVE OFFICER, DRUMWAVE, INC.

Ms. DENNEDY. Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for having me here today.

I am in the clean-up position. So I will not go deeply into the various analyses in my written testimony. I submitted to you, Chapter 13 of the Privacy Engineer's Manifesto, a book that was actually published before GPR was actually put into law but in the thick

of the negotiations, and many of these issues were pertinent then as I believe they are now.

As everyone you have heard reflected here is, I think the summation answer is this is hard, and we are not afraid of hard things, although Ranking Member Brown might have some cynicism around—I think it was you or Silicon Valley CEOs. I happen to be one. I am not like Mark in many different ways, but I assure you there is a lot of work that has been going on over the years.

I have spent most of my career first as a patent litigator and then as a chief privacy officer, as one of the first five in the world, where we decided and sat down in a small room together that there must be something better. There must be something bigger. There must be a way to functionalize what was then the only real framework was the OECD Principles for Fair Information Management and the '95 Act coming out of Europe. So we have very much been led in high tech in the belly of the beast by the Europeans for decades.

So what we did is really look at what is the functional tool. So just as Julia Apgar told us once upon a time, when there was a huge infant mortality, stop looking at just the mother and sometimes look at the baby. The procedural change of turning a nurse's head and looking at a child to see if it was breathing or not changed the child and the parent mortality rates.

We believe at DrumWave if you look at the data, we will have a similar moment.

If we indeed say value our data—"I proclaim that you must value the data. You must give an accounting, dear tech firms, dear hospitals, dear Senator bodies, of every single piece of information that is observed"—I will submit that you cannot today because the systems are designed to create more systems. The systems that we are sitting on top of and running our economies on and our cultures and our families and our educational institutions are based on software and hardware rather than data.

So the shift is how do we account for and look at data, and I go into some length in my written submission about picking a model. Whether it is a tangible property right, we have aspects of tangible property that are working, but some are not.

So, for example, let us look at a privacy right that is not necessarily a data privacy right. When I go into a public bathroom stall, for a brief moment, that stall is mine. I do not own that real estate. I do not even buy a ticket. I just go into the stall, and the expectation is that I close the stall, and it is mine for a moment. The moment I left, it is no longer mine.

So think about data moving in and out of cells, in databases, left and right. We may think that we want to understand every single transaction. What you actually want to do is find the errant transaction. So we are actually working on developing something that we are calling a "dynamic information meaning score," which is a combination of looking at the machine learning on databases and data systems as they do flow today.

So engineers, such as my father, with whom I wrote this book, understand back from the days of Univac and the earliest days, when you model data, when a real engineer models data, they think constantly about all users, the auditors, the lawyers, the

regulator, and the user. We have forgotten the user in this current economy. To look at the user, you must look at the data. To look at how you build systems, you have to think about who these users are. There are aspects of data if we ask the systems. We will find the answers, but I believe the model looks a little bit more like the constructs around intellectual property, where you may have a shared right.

In fact, the economic value for companies in a social networking concept is the grand value. So, ironically, if you wanted to get a payback of what your data was worth, it is actually worth less as an individual person the greater the dataset. The greater the dataset, the more the social network gets from the analytics off the top of it. So if we do a pure formula of how much each of us is worth, we will find a diminishing result.

If instead, we look to things like copyright and trademark and goodwill and brand, then we might find a blooming type of right. So the more I participate online as an individual, I actually am increasing the value of that transaction.

I will leave the rest of my remarks for question and answer, and thank you very much for your time and covering this important topic.

Chairman CRAPO. Thank you very much.

Each of you raise very interesting aspects of this issue.

I would like to start out with you, Mr. Ritter, and focus for just a minute on GDPR. The European Union's new privacy directive provides individuals with greater control over their data, including the right to access, erase, and restrict the processing of it. How does the European Union approach—how does the concept of data ownership show up in the GDPR?

Mr. RITTER. Well, thank you, Senator.

Many of the rights that you are describing are the things that we might associate as attributes of ownership to our computers, our cars, other things of physical goods that we own as consumers, who can use it, who can share it, who can possibly sell it on our behalf.

But the reality is that ownership as a legal concept has not been addressed in the GDPR. So we have this awkward situation in privacy law where these rights are being assigned to or being confirmed by legislation to exist for the individuals, but they have no mechanism of attaching those rights to the information.

In all other modern systems that we have in commerce, there is a concept of ownership, and I think that has been, as Senator Brown said, something that was skipped over, both in Europe and here in the United States.

By establishing ownership as a concept, nothing should degrade or reduce the rights of an individual, a data subject to be able to have awareness of what their information is doing. But what I think the Europeans did in GDPR revisions has been to create transparency, create awareness, create accessibility, all of which are consistent with the kinds of things that are being proposed in legislation such as the DATA Act by Senator Cortez Masto, and certainly the Own Your Own Data Act by Senator Kennedy.

So the Europeans skipped it as well, and I think that actually has created an opportunity for the commercial sector to exploit that

data without giving the individuals effective enforcement. And I think that is what is missing from GDPR. If we know who owns it and, therefore, who breaks the rules of their custody of that data for the individual, then we have stronger enforcement of those.

Chairman CRAPO. All right. Thank you very much.

Mr. Marlow and Mr. Rinehart, I think each of you, if I recall correctly, talked about the cost of privacy or, I guess, the cost of ownership if we create a system like that. Could you each just briefly expand on that a little bit?

Mr. MARLOW. Thank you, Mr. Chairman.

Let me say, initially, that I think that the concepts of cost and the concepts of ownership come in because of the familiarity of that model to Americans, right? I own my car. I own my television. I own my house. So the idea that because I have control over my car, if I own my data, that would give me similar levels of control, and so we think about cost as being part of that conversation.

But what I would remind the Committee is we have rights to free speech, even though we do not own our speech. We have rights to vote, even though we do not own our vote, and we have rights to privacy, even though we do not own our privacy and our data. So I would encourage people, although it is tempting to kind of come back to what is the value, the idea that because we see control elements in the marketplace and in private property, that if GDPR is trying to copy that level of control, it must also copy the marketplace model, including assigning costs, I think gets us on the wrong track.

Chairman CRAPO. Thank you.

Mr. Rinehart?

Mr. RINEHART. Yes. Thank you for the question.

This, I think, really fundamentally goes at kind of the heart of what consumers want. I mean, I know there are a lot of concerns, obviously, with what is happening in Silicon Valley and concerns about privacy, but we do know that consumers do benefit pretty massively from a lot of these services. And there is a lot of reports and surveys and information to that extent.

What I would highlight is that if you really do establish the property right and data where you are effectively requiring every single person to say yes to some sort of innovative service, the kind of new innovative services that you would want to compete with a Facebook or a Google might not actually be able to be created.

I know this is not exactly the—sometimes it is not exactly convincing to individuals that these sorts of things could happen, but we have seen these in the past. Especially with, for example, the telecommunication companies, they had a very similar sort of, kind of opt-in requirement whenever they were doing—in the 1990s when they were trying to reach consumers, and we do know that that did have an effect on some of the telecommunications companies, including U.S. West.

I would just highlight the fact that when you do require individuals to say yes to innovation, it just makes that sort of innovative service and products all that more difficult.

Chairman CRAPO. Well, thank you.

And, Ms. Dennedy, I am out of my 5 minutes, but I am probably going to ask you in writing to respond. You had some very intriguing issues that you raised, and I want to pursue those with you.

Ms. DENNEDY. Absolutely.

Chairman CRAPO. Senator Warner.

Senator WARNER. Thank you, Mr. Chairman. Thank you for holding this hearing. This is an issue that I am very interested in and engaged in. I agree and disagree with a number of the comments that have been made.

Mr. Ritter, I do think this America's failure to leadership in this area is going to come back and harm us. I think it is a pattern where we are seeing America start to retreat.

Mr. Marlow, I think you accurately point out some of the tensions of a traditional ownership model. It gave me a lot to think about.

Mr. Rinehart, I think you are a defender of the status quo, and frankly, I find your arguments very lacking because I actually think the status quo is not going to be continued. I find this notion of "Gosh, it is hard to figure out some of these ideas" is patently absurd.

I made some money in the telecom business. I remember, initially, it was really hard to figure out beyond user base what these companies would be worth. Well, the market drove a methodology around value, around spectrum, not imperfect. We came to that. Marc Benioff, when he lost out on the acquisition of LinkedIn, basically said, "Companies are buying these based on the value of the data that is being collected."

Ms. Dennedy, I agree there is a complexity to this. It is not single data points. It is that combination, but to make an argument that you cannot figure this out or it is hard to figure it out, it is going to be an unwarranted cost, that is just totally spurious. Companies are making acquisitions all the time in this space based upon valuations.

That is why I think one of the areas I would like to start with that I think there could be some broad bipartisan agreement—I got bipartisan legislation on this called the DASHBOARD Act that would say we ought to at least know what information is being collected on us in a more granular way. We ought to be able to know who that is being offered to on a third-party basis, and yes, even, Mr. Rinehart, if it is a little bit hard and we will not be a perfect model, but we ought to know what it is worth because the premise of these companies that have said, "We are offering you a proposition that this is all free," there is nothing free about what Facebook or Google offer. It is not morally wrong, but they are giant sucking sounds of personal data being collected about us, being monetized in a model that, based on advertising, there is nothing wrong. But there is so much opaqueness.

And, clearly, the establishment and established companies do not want more transparency because we might have—grapple with the questions that Mr. Ritter and Mr. Marlow put out so strongly, and we might actually—if we had more valuation questions, we might say there might be companies that would say, "Well, maybe there is a way to disintermediate between the platform and the user," because if we know Kennedy's data is worth $10 and Tester's is

worth $20 and mine is worth $5, maybe you might be willing to give some portion of that, maybe not even having to get to the ownership question, so that somebody could provide a level of service in between to help protect you.

So it is a hard, hard issue, but to say there is not any previous models, I think, is wrong. I think the notion that we cannot sort this out, I would urge—and I know Senator Kennedy has got some legislation in this area as well. I think it is really, really important that we do the hard work of trying to sort this out, particularly whether we are thinking about consumer protection, whether we are thinking about the idea of true transparency, whether we are thinking about the idea of pro-competition.

Unlike some of my colleagues who want to go straight to breakup, I would rather see if we can introduce more competition into this model, and we are not going to have more competition if we have the level of opaqueness in where the large platform companies control all the data at this point and are not anxious to share, are not anxious to have more transparency continue that way.

So I would like to start—I guess I am a little more speechifying than questioning here, but, Mr. Ritter and Ms. Dennedy, talk about the idea around digital markets, about the notion—without getting to ownership, but just the notion of more transparency, value add, value less. Either one of you want to go first?

Ms. DENNEDY. Jeffrey knows that I am obsessed with this area.

There is a great deal to be gleaned, earned, and profited by through transparency. I am a huge, huge fanatic and fan. In one of my prior companies, I did—with the consent of the Federal Trade Commission, I did a graphic novel for our privacy policy for Intel because I believed the subject matter was too complex to read through 16 pages of legalese.

So we did a cartoon to train our customers. At Cisco, we did what I called the "Lord Ashfields." We did subway maps that look a lot like the underground in London to map out where the data is, where was mine, where was yours, where was third parties. Was it perfect? No. those maps are proliferating.

Actually, ironically enough just this week, I heard from some of the privacy engineers at Facebook that they are adopting them. I do not know if that is going to bubble up to the top, but I am pleased to hear that the beginnings of that innovation are occurring.

I think transparency allows you to understand where asset—I go back to the old-fashioned accounting rules and say, "What is an asset?" It is something based on an activity that can potentially provide benefit in the future, and if it stops providing future benefit for the consumer or the user, it starts to become a liability. That sounds a lot like a market.

So the more transparent, I believe, that we can be and create the systems to look at the metadata that we have already, we can start to create those markets.

Now, I am a believer in this, but I am also early in the market. Is this something comprehensively that if you said tomorrow, we want abject transparency, it would take some time to catch up? I think we can get there.

Chairman CRAPO. We will probably have to have your remarks, your answers, Mr. Ritter, in writing or following.

Sorry, Senator Warner. We have got to move on.

Senator Kennedy.

Senator KENNEDY. First, I want to thank all of you for coming today. I know you are all busy, and I do not want you to construe what I am about to say as a comment on your personhood. It is more a comment on the testimony.

I am not fluent in BS, and I have not the slightest idea what you are talking about, except that we have got a problem.

One of the issues before us is whether data is property or not. I did not hear you answer that. If it is not property, it is something, and a lot of people are making money off of it.

Mr. Rinehart, you said it is hard to value this something. Well, let me tell you one way to value it. Last year, Facebook's revenue was $56 billion. That is nine zeroes. 98.5 percent of it was revenue from ads that were specifically targeted to people based on data.

Mr. RINEHART. Yes.

Senator KENNEDY. So whether it is property, a property right, or a cabbage, it is being monetized, and it is people's personal information. Can we agree on that?

Mr. RINEHART. I would want to add a little bit of complexity to that, that——

Senator KENNEDY. Of course, you would.

Mr. RINEHART. So, I mean, what they are selling is the—effectively, the attention of individuals, and that to me adds some complexity to this question about the value of data as compared to, say, the value of attention.

Senator KENNEDY. Mr. Rinehart, I do not mean to be rude, but we are Senators, OK? Whatever—this is what I sense, and I have nothing against social media. These are wonderful American companies, but we are dealing with problems that nobody anticipated, at least I did not, and my constituents did not.

Forget about whether it is a property or not. It is something, and it is mine, or at least it originates with me. When I go on Facebook and share information, whatever you want to call it, it started with me, and now it is on Facebook and whoever Facebook chooses to give it to.

Why can't we have a rule that says, whatever you want to call it, my rights follow it and I can license it, share it with you and Facebook—I hate to pick on Facebook, but that sharing has to be knowing, and it has to be willful. And I have to be able to change my mind, and I have to be able to call Facebook or click on an icon and say, "By the way, I want to see what you have got on me." And consistent with Senator Warner's point, I would kind of like to know what it is worth. Why cannot we do that?

Now, I am going to tell you what part of we cannot—reason we cannot do that. Part of that is our fault. We have been holding hearings on this subject—I do not know—2, 3 years. We will probably be doing it again. This is not a reflection on this Committee. This is on the Senate. All we do is issue press releases, hold hearings, and strut.

This to me is not complicated. Why cannot we just agree on those rules? What is wrong with that?

Mr. RINEHART. I would not necessarily say that those rules are wrong by any means. I mean, CCPA, California's Privacy Act, does, in fact, establish a lot of those sorts of rights without having to establish a property right. So that to me—I mean, we can—and I have been supportive of privacy laws in the past, and I think that that is something that is very much needed for this country.

Senator KENNEDY. Yeah. But you all keep saying that, and then you never propose anything.

Look, I am about to run out of time here. Let me tell you what is going to happen. We have got a problem. I do not think anybody anticipated it. If they did, they did not do anything about it. At some point, the American people are going to get fed up, and then we are going to have to do something. Otherwise, we will not get reelected, which is what motivates people around here.

Mr. MARLOW. Senator, can I just suggest one thing?

Senator KENNEDY. And you may not like what we do.

Mr. MARLOW. Fair enough, sir, but if I could just suggest one thing. If the Senate were to pass very strict privacy laws that did not necessarily adopt a data property model, people with the right to say you can and cannot use my data would still be able to sell their permission. They could still say, "For $10, I will give you a yes instead of a no." So it is possible to have people sell their data without adopting the data's property model that carries with it a lot of downsides that strong privacy protections that do not necessarily impinge the right to sell data would not bring with them.

Senator KENNEDY. I am way over. I am sorry, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Menendez.

Senator MENENDEZ. Thank you, Mr. Chairman.

Mr. Marlow, companies such as LexisNexis Risk Solutions collect hundreds of nonmedical personal attributes in order to help to predict a person's medical costs. The company claims that providers can use this data to improve patient health care and health outcomes, but I have concerns that this same data can be used to discriminate against patients, including vulnerable populations such as low-income individuals and the elderly.

What, if any, protections exist for consumers to prevent insurance companies from using this data to discriminate against customers?

Mr. MARLOW. Thank you, Senator.

First of all, I want to recognize that you point out a very particular challenge. The healthcare data area is something that will have to be explored and drilled down to independently, regardless of where the Senate comes out on this issue, because certainly I think concepts of having people be able to study populations and develop healthcare solutions and cures to diseases is something that is very, very important.

I think the challenge is that when data flows into a marketplace, slows into the insurance companies, it is very difficult to be able to parse the algorithms, to understand to what extent they are——

Senator MENENDEZ. So, in essence, you are telling me that there is no patient protection at this point?

Mr. MARLOW. Well, I think that there are certain laws that would kind of *writ large* propose kind of blatant discrimination, but

it is the finer discrimination that is hard to identify, that is hard to get at.

And so the question of—without, unfortunately, probably the answer you want—algorithmic transparency is a very challenging one, but it is within that question that an answer may or may not be revealed.

Senator MENENDEZ. Ms. Dennedy, after data companies analyze this data and generate a health risk score for a client such as a health insurance companies, do consumers have any right to see that analysis or score?

Ms. DENNEDY. I think that they should, if they do not already. I think this is, part and parcel, of what we call "privacy engineering" and the new field of ethics engineering that is emerging, and this is exactly addressing these complex issues that you are talking about. When you are actually doing system design, the question must be asked. How do you interrogate how decisions were made?

In the same light, when we are talking about ethics engineering for machine learning and machine algorithms as everyone is kind of calling, colloquially, "AI" these days, most of it is machine learning. Understanding for patients where the algorithm has been applied may be nonsense to that patient. However, to the ethics boards of hospitals today to the FDA that approves drugs and gadgets that are part of our healthcare system, I believe there are structures in place if we provide the transparency behind how these scores are calculated.

Senator MENENDEZ. What happens if some of the data is wrong?

Ms. DENNEDY. Well, that is exactly the problem.

Senator MENENDEZ. What recourse do consumers actually have to correct inaccurate data that is going to affect their health profile and their risk that ultimately is going to affect their insurance coverage and other things?

Ms. DENNEDY. So this is part of the beauty of what is included in the GDPR that we would love to see in a Federal bill, which is the privacy disclosures, the privacy impact assessments that must be done before a system is put into place to process information or when that system is changed by third parties, that information would be in those disclosures of those privacy impact assessments that are required under the law in Europe and not here.

Senator MENENDEZ. I see Mr. Ritter is anxious to give a comment.

Before he does, let me throw out what probably will be next to my final question. Given the sensitive nature of health data, does that data deserve heightened protection and/or regulation?

Do you want to start off, Mr. Ritter?

Mr. RITTER. Thank you.

First, I would take exception to the notion that health data can be treated apart from the broader questions, both the personal information and all information that we gather. We need solutions here, and with regard to how we enforce these rules, as a Government, we must demand transparency.

I watched with interest, the hearings of this Committee earlier this week on the audit process and looking at brokers and the SEC rules, and that kind of transparency of automated awareness, automated surveillance of compliance is going to be what we as a

Nation must anticipate. We can no longer just write generic rules that tell companies what they should and should not do.

The consumer benefits from that level of interaction in enforcing rules by being able to see that from an automated perspective.

One of the earlier references was to the provision of Oregon law about having a unique tracer on a record. That is exactly how it is done today, and I actually think that is where we are moving in the future.

We have license plates on automobiles. We have serial numbers. We have RFID devices. I put one inside the box of my bicycle when it ships across the ocean, so I know exactly where my box is, no matter what the airline says. That kind of traceability is getting smaller and smaller, and I think that is going to be part of how we can enforce the rules is asking the machines to execute the compliance with those capabilities.

Senator MENENDEZ. Mr. Chairman, this is a big topic, but I think, particularly, we are being naive if we simply assume that the collection analysis health data will be used only to lower costs and improve health outcomes. We have to take seriously the threat that this data could be abused and ultimately lead to consumers being taken advantage of, and I look forward to working with the Chairman.

Chairman CRAPO. Good point.

Senator McSally.

Senator MCSALLY. Thank you, Mr. Chairman, for having this hearing. Thanks, everybody, for their testimonies.

I first need to confess, like I am a privacy zealot. Personally, I lead a very boring life, but just on principle, I am the kind of person who fills out those forms when you get them in the mail about opting out from your credit card company. And I do not put location services on my phone. I do all sorts of other weird things that I want to let everybody know about it.

And I always have these conversations, extremely frustrating to me that we are in this situation that we are in. I have arguments with one of my staff members who like loves tailored ads and does not mind giving up all his privacy in order to have tailored ads, and I am like, "I will pick what I want to buy. I do not need you gathering my stuff and sending me ads. It is just like it is such a personal frustrating thing for me and for my constituents that I represent.

And I appreciate it is a complex issue, and what I am hearing from you all today, maybe data as a private property maybe is not the way to do it. OK, fine. But I guess what I am struggling with is part of what has happened, I think, culturally, is we have got all these new tools that are out there that people are able to use for free, and their revenue model is to collect your data and sell it. I mean, we all know that, and maybe, unwillingly, people did it initially. But now that is kind of our expectation that we can do a free internet search. We can do free social media contacts and communication. It is not free because it is taking your information and profiting off of that.

But if there is another model of like, OK, is the market not demanding this, I guess, where we have a social media platform where you can pay a certain amount and say, "I want to be able

to engage, but I want to keep all my stuff private, so you cannot sell it," what is the value of that, and is there even a market for that?

Mr. Rinehart, on page 7 of your testimony, you said during a study, most subjects happily accepted to sell their personal information for just 25 cents. Part of this is kind of cultural on what our expectations are.

I would also be concerned about the socioeconomic divide. So if some of us are willing to pay in order to protect our privacy but others cannot, then we have a division going on there of just those of the lower income having their data being taken and sold, and that is a problem too.

So if the solution is not data as private property, what is it, and does it start with transparency? That is where I am sort of landing. Does it start with let us shine a flashlight on what is actually going on, let people see and be mortified by what information they have that is being collected and analyzed, and then maybe that will help drive a different market solution or even different companies?

I mean, I am not one that wants a Government solution that is going to stop innovation. We want less regulations and more innovation, but in this case, how do we deal with that conflict, and what is the best place to start? Is it transparency?

You guys are all saying it is not data as private property. Then what is it?

Mr. RITTER. Yes. Transparency is critical.

What we are seeing in the way we manage data as property is increased detail, increased capability of managing detail, and that also enables us to have more rapid response both in corporate systems, in government systems, in information security, allows us to see what is happening.

Transparency is good, and the division between you and your staffer with regard to the acceptance of all this is something we are just going to live through as they——

Senator MCSALLY. But then we get to choose. It is all about freedom, right?

Mr. RITTER. It is humankind.

Senator MCSALLY. Yeah.

Mr. RITTER. Right? But for the systems to survive and for the digital age to not bring us down but actually to be a backbone for humankind to move forward, we have to demand that transparency in Government requirements, such as the ones that are being proposed in Senator Kennedy's legislation and some of the other pieces that have been drafted by Members of this Committee are outstanding first steps in that direction.

Mr. MARLOW. Senator, if I may—and I really appreciate being able to discuss with a privacy zealot like myself.

Senator MCSALLY. Yes.

Mr. MARLOW. But a couple of things. So, one, privacy is not about secrecy. It is about choice, right? And so it is certainly acceptable within a privacy regime for you and your staffer to come out in different places.

Senator MCSALLY. Exactly.

Mr. MARLOW. But what we want to make sure——

Senator MCSALLY. But right now, there is no choice for people like me.

Mr. MARLOW. Precisely. And we want to make sure not only that you have a choice——

Senator MCSALLY. Yeah.

Mr. MARLOW.——right? But that the choice is well educated, informed, transparent, meaningful, and precise. All those things, I think, have to enter the equation.

Another aspect that you brought up that is important to privacy is that we want to make sure that consumers like yourself and myself cannot be punished by companies——

Senator MCSALLY. Right.

Mr. MARLOW.——for exercising our privacy situations, or conversely, that those who give up their privacy are rewarded in ways that we are not.

But I think that the idea of bringing money into that equation goes to your final point, which is we do not want to establish a system like data-as-property where Government is used to put additional weight on the anti-privacy side by saying, "And we are going to make sure you know there is money, although we may not tell you how much, but there is money at the other side of the equation."

So I thank you very much for your observations. There is absolutely a path to get there.

Senator MCSALLY. Well, I know I am out of time, but eventually, money is a part of it, whether it is monetizing your data or not. There is no such model for Facebook to exist if we are all opting out, right? Because they do not—they cannot—that is not their business model.

So somehow—I mean, I know we got to go, but somehow we have got to have this conversation about how some of these tools can be accessible for people that really can be impacting their lives. Forget about the social media aspect, but even in medical advances, but also having people know what is going on with their information and why it is being used.

Mr. MARLOW. Right. But like your staffer, Senator, not everyone is going to opt out. That is kind of a dooms-day scenario, but that is not going to happen because some people do like targeted ads and like to be directed online.

Senator MCSALLY. All right. Thank you, Mr. Chairman. I appreciate it.

Ms. DENNEDY. Can I just have one more quick——

Chairman CRAPO. Real quick.

Ms. DENNEDY. Thank you. Very quickly.

I think we are focused on transparency at the bottom lawyer. Let us not forget the top. The war that is going on for every CPO right now, the war for attention in the budgets, I do not see any CPOs sitting on public boards. I do not see the Chairman's letter to their shareholders talking about what their data scores are. Until we score our data and it comes from the top down, it is entirely a battle of one, and it depends on who you privacy officer and how big her hairnet is. I do not know what the appropriate senatorial thing is to say there.

Chairman CRAPO. Understood.

Senator MCSALLY. Thank you.

Chairman CRAPO. Senator Tester.

Senator TESTER. I want to thank you, Mr. Chairman. I want to thank Ranking Member Brown for having this hearing. The more that is talked, the more confused I become.

OK. I mean, I deal with property the same way most people deal with property. It is something you own. It is something you sell. A bushel of wheat, for example, I am a farmer. I sell it. It goes to General Mills. General Mills might sell it to somebody else. They might make flour out of it, but I do not care. I got my money, and I do not give a damn.

The problem here with this and why it is such a critically important issue and why this hearing is so important is because the solution is so complex because everybody has got a different perspective.

Senator McSally said it. She loves her privacy, and not secrecy, but privacy.

So we have got a situation where we have got health information that if it gets in the wrong hands, it can have incredibly—or even in the right hands, I might add, that can have incredibly negative impacts on my health insurance premiums; bank information that could cost me to buy a house a lot more or a lot less, or health premiums, same thing on the health premiums.

And then we have got a situation where I buy a transmission for my combine, and who really gives a damn? Really, I mean, what are they going to do? I bought it. It is done. All that information can transfer. I am not going to buy another transmission because I do not need it.

So it is really hard to figure out where we are in this and what works, but let me ask you this. And I have a great respect for everybody that is on this panel, and I mean that. I appreciate all of your perspectives because I think they are very interesting. But we had a hard time with REAL ID in Montana. If we put tracers on information, Mr. Ritter, should my constituents be concerned about me voting for a bill that has that in it?

Mr. RITTER. Yes, but not because of the tracers, but because the inadequacy of the bill to not deal with the consequences of the records those tracers produce. That is where the difference can be made.

Mr. Tester, my original clients 40 year ago were farmers.

Senator TESTER. Yes.

Mr. RITTER. And so in response to your point, actually when you bought the new transmission, that fact is very interesting to the company from which you purchased the oil because it wanted to know the useful life of the transmission. The transmission company wants to know, one, you purchased it based on the number of hours of usage.

Senator TESTER. A really good point.

Mr. RITTER. Number of hours of usage that created off of the tractor.

Senator TESTER. And so the issue becomes should we pass a bill that says, basically, you cannot——

Excuse me. If this is my wife——

Mr. RITTER. We all understand.

Senator TESTER. It is not.

You know what? You know what this is? It is a targeted ad.

Mr. RITTER. It is a scam likely.

[Laughter.]

Senator TESTER. So you want to talk about cost and money—do you want to talk about cost and money? I mean, if there is one thing that makes my head explode, it is the fact that I got people out there who I do not want to do business with that are trying to market crap to me that I do not want, and whether it is through this telephone or whether it is through the computer when I am sitting there trying to read an article and all these damn screens keep popping up—and I am not a tech genius to get all this stuff off, it is baloney. And that is the real problem for me. It may be a different problem for somebody that is in a different economic stature, but the problem for me is I am getting all this information I do not want. So how do we fix it? is the question. How do we really fix it and protect my civil liberties for privacy, not stop business? But I would tell you that several of you talked about cost. There is a lot of cost with doing nothing here too. So we need to do something.

So how do we fix it? Because I got the impression from you, Mr. Ritter, that the European Union is doing—and other people, by the way. I do not want to pick on you. You are a good guy. The European Union is doing some stuff, and Japan is doing some stuff, but it is really not complete, or is it?

Mr. RITTER. One of the things that distinguishes both European policy development and Japan is extensive research and consensus development before they introduce definitive rules. That is something we struggle with here in the United States to stay in the——

Senator TESTER. So what did you just say?

Mr. RITTER. They think about it, and they write their rules with design.

Senator TESTER. OK.

Mr. RITTER. All right? You would not buy a combined——

Senator TESTER. That is exactly what we do here in the U.S. Senate.

[Laughter.]

Mr. RITTER. A survey came out just about 8 weeks ago on the impact of GDPR on the European citizen, and it indicates that they have had over 145,000 complaints just in the first year. But—and I will take a look at my notes here—45 percent of the people that were surveyed in Europe liked the reduction in nonresponsive marketing. They were getting better tailoring, and they liked that.

Senator TESTER. And how did—excuse me. I am going to make it very, very short. How did they stop that reduction? How did they make that reduction in marketing happen?

Mr. RITTER. Many of the rules that the GDPR embraced, which also, I think, Senator Cortez Masto's bill embraces, just put an accountability on companies for having to disclose the use of——

Senator TESTER. And what happens if they do not follow the rules? Are there penalties?

Mr. RITTER. The problem of enforcement is one we also have to address.

Senator TESTER. I get back to my original point. If this was easy, it would already be done.

Thank you, Mr. Chairman. Thank you, Ranking Member Brown, for your courtesy.

Chairman CRAPO. Thank you.

By the way, we have a Do Not Call List bill that we are working on.

Senator TESTER. Yeah. Well, we passed it, did not we?

Chairman CRAPO. Well, we have a better, more enhanced one.

[Laughter.]

Chairman CRAPO. Go ahead, Senator Toomey.

Senator TOOMEY. Thanks, Mr. Chairman. I think this has been a great hearing and a great discussion. I appreciate you doing it, and I want to really thank all of our witnesses for contributing to thoughtful ideas to a very challenging and interesting conversation.

Some of the points, I think, that are extremely important, I think Senator Tester was touching on the fact that probably most people have different views about different datasets about themselves. I mean, I want much more privacy about my healthcare records, for instance, than I do about whether I just bought a tractor.

I am sympathetic to the argument that transparency is generally, probably a good thing, and I am sympathetic to the idea of consumers having greater ability to exercise some choices about what data is released and what is not.

But one of the things we have not talked a whole lot about this morning is the fact that in the model that has organically evolved, consumers get compensated. There is actually a lot of compensation. We talk about how much revenue Facebook took in. It is a staggering number.

It is hard for me to quantify, but I can tell you I perceive significant value every single day when I go and turn on Pandora. I can get to listen to any music I want for free as long as I want, and very regularly, I will go to any number of competing map software and get fantastic direction to any destination I want to go to anywhere. And I pay nothing for it.

I can read newspapers and magazines. The list is endless, right, of all of the things, and in fact, in many of these spaces—not all—many of them, there is real competition. To the extent that there is real competition, you have to assume that the data that is being—that is the revenue stream for these companies that have these apps, they are competing for that. And so they are presumably competing to offer me ever more in return for me providing them my data, to the point where it should converge on something approximating the value of it.

So I like that value. I love the innovation. I have no idea what new things are going to be available next year, but I bet there is a bunch of others that I am going to enjoy using.

So I wonder if anybody—let me start with Mr. Rinehart—would want to comment on the fact that without property rights, which I have not thought enough about to have an opinion on—consumers are already being compensated every single day for the data that they share. What are your thoughts on the level of compensation?

Mr. RINEHART. Yes. I mean, this is something I tried to highlight in my testimony is the conflict between the data that supports the

services and how consumers then value the services because those are slightly different things.

We do know that consumers do value these services pretty extensively. I did some quick calculations before the hearings, and social media, by most accounts, probably benefits people to about $13,000 per year. They use it pretty extensively. I can follow up later. But we also know from a whole bunch of other surveys that if you were to try to give up, for example, Google search, it would cost people something like $18,000 per year to be willing to pay to get—or to be compensated to not use Google, similarly like $8,000 or around $8,000 for maps, as you had mentioned, or mapping services.

So, yes, consumers do benefit in kind of these implicit values or in an implicit way, which does not show up in a lot of data, and that is also what makes the valuation of data itself. And as I mentioned throughout my testimony, it just makes it a little bit more difficult.

Ms. DENNEDY. Can I add one thing? My ears are hurting that we are saying it cannot be a property right. I think that data is probably some sort of an intellectual property right. It may not be a tangible right, but I think exactly as you are talking about, data to me is currency.

So if you think about a penny, a U.S. penny, that alone is not very much, and I can tell you I have got a penny had you have got a penny. The story that that penny tells when you put it together with the rest of my data story—where am I spending it? How am I spending? Who am I? If I hand him a dollar, it means less than if I have a dollar based on our past history.

So when we are talking about valuing datasets, let us be careful to understand that what you are really talking about is the lifetime. Sometimes there is a one-time transaction with data, and it looks and feels like a property right or a bailment. And other times, it really is "What is that relationship worth?" And the banking community, in particular, understands that better than anyone.

Mr. RINEHART. Can I just add one small comment? I mean, I would mention at least within intellectual property, the traditional reason why you establish property rights for intellectual property is because there is an underproduction of those sorts of services, and what we are talking about here, especially with privacy, is very much the opposite of that. What we are trying to establish or at least what we are trying to talk about is the limitations of disclosure.

I just find the intellectual property, the typical way of talking about it and the typical way of thinking about it through property rights as a way to incentivize creation is, in fact, the opposite of what we are talking about with privacy, which is incentivizing some sort of disclosure, which is just, I think, a complicated—it is a more subtle way to think about the difference between the two.

Senator TOOMEY. Thank you very much.

Chairman CRAPO. Thank you.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman. Thanks for your flexibility. The Finance Committee was doing a really important hearing on opioids, and as Mr. Ritter knows and some of you know,

it is a terrible problem in Ohio. It is one of the worst problems in the country.

We know the system we have right now does not protect Americans' privacy—phones, laptops, TVs, credit cards—turned into tools to harvest personal information for a few or maybe more than a few to profit.

Mr. Ritter or Mr. Marlow, when we are talking about a property rights model for data, is not that just a way to legitimize and expand on the way Facebook and other big tech companies spy on every aspect of our lives?

Mr. RITTER. In the 21st century, Senator, surveillance will be part of our life. This is something that we as a society must decide how to regulate.

I do not think that they are spying on our lives in a way that is, at first instance, inapposite to our purpose in interacting with them. I walk into a bank to open a bank account so that I can save my money and pay my bills. I roll onto a gurney into a hospital ER for them to save my life, and that involves collecting a whole bunch of data and X-rays and MRIs and vital information. This is part of how we provide services in the 21st century.

Each of us, to use your metaphor, is a data generator, even our devices, and I think that what we have to recognize is that we cannot stop the surveillance that the digital age demands for operational efficiency. But we can impose appropriate rules against the misuse of that information beyond the original purpose for which it is collected, and we can better enforce those by making clear who stands responsible.

Senator BROWN. Thank you.

Mr. Marlow, answer that, if you would, in however direction you want to take, but include in it explaining how a property rights model would or could or should provide meaningful privacy protections.

Mr. MARLOW. So I would say this. The property rights model would provide privacy protections, and the fact that any model that says you own this data, you have the right to sell it, the corollary would be "And you have the right not to sell it."

The problem with the data property model is you can accomplish all those things with privacy legislation, like California has, like Maine has, without having to create a data property model that will further incentivize people to give up their property.

And I would say, just to put a fine point on something, surveillance is not necessarily going to be a part of our lives going forward. Attempts to surveil us will be. The extent to which surveillance succeeds or fails, the extent to which we have privacy or not is in your hands.

I would be more than happy to come back another time for this Committee to talk about the way that our laboratories of democracy, our State legislatures are approaching this issue and making significant progress.

So I would not be defeatist here. The only way that privacy disappears and surveillance wins the day is if we take an attitude that it is inevitable.

Senator BROWN. Let me pursue that again with both of you, Mr. Ritter and Mr. Marlow.

We have been discussing whether or not we should create property rights in data. I know that you both are skeptical that it is even possible.

Senator Kennedy compared data to a cabbage. If I sell you a cabbage or house or a car or any other property, I have to hand it over to the property owner. I sell you data. I still can keep a copy of it. How does the difference between data and Senator Kennedy's cabbage make it hard to exercise privacy rights, the same way you could exercise property rights?

Start with Mr. Ritter.

Mr. RITTER. Actually, I think cabbage and my medical record are very similar, Senator.

As detailed in my written testimony, the scientific consensus surprises us. In contrast to what Ms. Dennedy said, I do not believe information is intangible. It is a tangible object. It is just small. And as our technology evolves, we can, in fact, manage the rules and the use and the economic implications of that use through technical means and through rules being applied. We just have to design the rules correctly.

So I actually do think there is a great potential here to improve the protection of the individual from misuse and increase the enforceability of violations of those rules by making more clear, if you will, who is on first and has the ownership responsibility to make sure the consumers' interests are protected.

Senator BROWN. Mr. Marlow, comments?

Thank you, Mr. Ritter.

Mr. MARLOW. Data makes terrible coleslaw, unlike cabbage, so I would start there.

[Laughter.]

Mr. MARLOW. But I would say, again, the problem is that it feels like we are trying to put a square peg into a round hole. The data-as-property model, although it has some facets that promote property, also undermines property, like the need to—if you had data or a cabbage, that could be replicated indefinitely and passed around, the need to track it everywhere it went, so people could be paid every time they consumed a new cabbage or piece of data. And that would require the tracking of any information.

I could post something online that gets linked to my computer. Therefore, it provides personal information, and now my speech is being tracked all over the internet.

So, again, I think that if you want to focus on privacy, you should focus on privacy protections that do not have such obvious downsides that come along with them, and that is the data property model.

Senator BROWN. Thank you, Mr. Chairman, for allowing me one more question.

Again, this is for Mr. Ritter. I know you well enough, many years ago, to know you care about the wealth gap in this Country, and it is getting worse. We cannot continue to have an economy, although the Senate does nothing to fix this, that divides Americans into the haves and have-nots.

With that in mind, would a system of data ownership create a world in which the rich could afford to keep their data private, but those who—Senator Crapo and I have talked about the challenge

for low-income people and the temptation to sell all of those things. Would this mean the rich could afford to keep their data private, but too expensive or difficult for everyone else?

Mr. RITTER. People that are underprivileged or financially disadvantaged sell their blood to be able to put food on the table for their children, and I do not think we can escape the likelihood that they would also sell their data if there was an economic return that would be useful.

The bigger problem, of course, is to reduce the inequality, and we do that by being more visible of how that money is being made.

For all the comments that have been made about the cost of compliance, there are very few advocates that assert the objection to the cost that do not knowingly talk about the revenue, and when we realize how much money is being made by these corporations from the personal information without returning that back as part of the ongoing transactional relationship with the individual, we are making a mistake and improving the inequality.

Senator BROWN. Could Mr. Marlow answer that too? And then I yield.

Mr. MARLOW. I would just quickly say that blood is a replenishable resource. When you sell your privacy, it is gone, and I think that if I were to say to any Member of this Committee, for $50, would you sell me your most intimate, private, personal information, you would say no. But if you could not put food on your kids' table, if they were getting bread and water for the third night in a row and I said, "I will give you $50 for your most personal information," I would venture a guess that you would all say yes. I am not certain that that is what we want privacy to look like in this country.

Chairman CRAPO. Thank you.

Senator Tillis.

Senator TILLIS. Thank you, Mr. Chairman.

Thank you all. I think you have given us all a lot of good information to work on.

You know, I am somewhere between Senator McSally and being a privacy zealot and Senator Toomey who has rightfully pointed out all the benefits of using this data responsibly.

I think that Congress—and I am curious, and I have got a couple of questions for you that may to down the line. But, one, Mr. Marlow, I hear you talk about the laboratories of democracy. I believe in it. I was the Speaker of the House. I loved the kind of stuff that I was doing in North Carolina.

But I am concerned if we do not come up with a Federal solution to this problem that deals with data breach, data privacy, and data ownerships, then we are creating a patchwork of lies that is going to make it more difficult for American-based innovators to really produce the next generation of value-added. Is there anyone here who thinks it is a bad idea for us to pursue Federal preemption and take on those three buckets?

Mr. MARLOW. I do, and the reason I——

Senator TILLIS. That is why I asked you first.

Mr. MARLOW. Thank you, sir.

[Laughter.]

Mr. MARLOW. So the reason I say that, to be simply practical, is this. The idea that the U.S. Congress would pass strong privacy laws that would set a reliable privacy floor for the entire country is exceptionally appealing.

The idea that Congress would come in where some States have passed even higher privacy protections for their citizens, like North Carolina might, and then say we are going to bring that privacy ceiling down to the Federal level, I find less appealing because I, like you, Senator, believe in our Federal model, believe that the States have the ability to—you know, you may have North Carolina passing a privacy protection that turns out, as we let it exist in the world for 10 years, serves to be a guiding light for Congress. But if we squelch it through preemption from the very beginning, we will never learn the lesson from your State, and so that is why I am very hesitant to have Congress creating a ceiling on privacy rather than a floor.

Chairman CRAPO. Others down the line?

Mr. RITTER. Thank you.

For nearly 30 years, I interacted on behalf of this country at the United Nations to write the rules that have enabled global electronic commerce to now thrive. There is one essential truth of global communication systems—uniformity rules.

Whoever writes the rules first usually wins that game, and our failure to be more proactive in addressing the valuation of personal information and all data has handicapped our competitiveness.

Having 50 different States is going to be adverse to our interests and, in fact, does not allow us to thrive.

Senator TILLIS. I want to move on to some others. I have to say that, in full disclosure, at Pricewaterhouse, I was a partner in global sourcing, strategic sourcing, and data analytics and data privacy and worked on it quite a bit. I actually think, first, we have to get Congress better educated on the issue so that we really know what we are talking about.

But I tend to believe we could be the jurisdiction that sets an international standard, that we may miss a few nuggets in some of the States that are doing good things, but at the end of the day, if we do not get this right, then the States that are laggards are going to expose their constituents and our innovation opportunity may be lost for the United States.

We have to understand that they are going to be aggregating data across the globe, and if we set a standard, we may be better off as a result of doing it.

Look, because I have been in technology all my life and I am still trying to teach all these young folks that work for me how to use it, when I want to be private, I go into incognito mode. When I do not want somebody to know where I am, I turn off location services, or I use VPN. When I see a platform that I do not want to share my data, I do not. When I see a platform that if I do share my data, I may be able to drive down the price point of something I am purchasing by 50 percent.

There is a website out there now where I can go put something that I want to buy. It aggregates all of the online retailers, and over a period of time, I say when you see a price point at this point, let me know and I will buy it.

When you talk about narrowing the wealth gap, I think there is a great opportunity for the people who have the least amount of money to benefit from these tools, if we get them right, to drive down the cost and drive down the cost to the consumer.

We now have someone that may be growing up in the trailer park that I grew up in, in Tennessee, that can get on a phone an drive a price point down. That used to be only available to large corporations that did strategic sourcing and had access to the tools, but we have really got to educate people on the various layers of data that we are talking about here.

Tom Tillis and all of my personal information, I believe, is mine. I may allow someone to take it and use it. I want there to be a very clear authorization there, and I want to know whoever has it will then ultimately have a responsibility for any kind of data breach or misuse of that information. Those rules of the road need to be defined.

But then we have to talk about the abstractions of data, where my identity is less important than my demographic, and then the aggregation of data that you actually use to gain insights and then target. I mean, all of that, all those layers of information have different implications in terms of whether or not I own it or whether or not my behaviors are just making it easier to find people like me that say, "Hey, you may be able to get what you are looking for, for half the case, based on your behaviors."

We have got to better educate Congress on what layer we have to protect and what consequences there are for platforms who fail to be good stewards of the data, but then recognize that these data models are also what are driving innovation that ultimately benefit consumers and I think will ultimately benefit patients in health care. That is the sort of stuff we have to work on.

And in Congress, Mr. Chairman, I know right now we have got at least three committees that think that they have ball control over this issue. One of the things that we have to do fairly quickly is figure out how we come together—and this has to be very task focused—and have each of these committees come together and figure out how to approach this on a more holistic basis, or otherwise we are going to keep talking about it and not act on it.

Ms. Dennedy, I think it is remarkable that you wrote a book with your dad on data privacy manifesto. I am going to get one. I am going to get a copy of that book, but what I would also like to get is the graphic novel that you were talking about, some of the other things, if they are publicly available.

Ms. DENNEDY. I think Intel has taken it down, but I will get you a copy, Senator.

Senator TILLIS. I think that that would be very helpful because that is the sort of stuff that we need to get out to the individuals so that they understand. You use the one as the underground, the map to show, so that you can very quickly say that when I opt in or if I opt out, an informed choice in that.

Ms. DENNEDY. Those are public. You can find them on *trust.cisco.com.*

Senator TILLIS. I will go through that, but I think all of you made very valid points. What we have got to do is synthesize it and, I think, come up with a data breach, data privacy, data

ownership policy that could potentially set a standard. We can be instructed by GDPR. We can be instructed by California. We can be instructed by a dozen or so other States that are considering it. But I think at the end of the day, this is something that Congress is going to have to take on.

Thank you all.

Mr. MARLOW. Senator, if I could just say one point. You actually, I think, perhaps inadvertently made a very strong case additionally why we need privacy laws. You mentioned that one of the ways that you protect your privacy is by using incognito mode. Incognito mode, despite its name, is not private. It basically means it is private for your computer and other people in your household.

Senator TILLIS. Right.

Mr. MARLOW. But if you search on Google, Google can still see where you are going.

Senator TILLIS. Right.

Mr. MARLOW. So that is part of the point. We need to make sure that not only that the Congress is educate but consumers are educated and actually have meaningful rights in the area.

Senator TILLIS. Absolutely. And there is a lot of other—there needs to be a suite of tools available to the consumer that can basically counter everything else that is going on after you hit enter. I get that. I think that is a part of the discussion that we have to have.

I just, for one, think that I have been in Congress now for 4 ½ years. We have been talking about this 4 ½ years. We actually need to take action, and we need to do it on a multijurisdictional basis. And we will continue to value your input.

Mr. Chair, the only reason I went over is I was the last person, so you are the only one I inconvenienced. And I am sorry about that.

[Laughter.]

Chairman CRAPO. That is the only reason I let you keep going too.

Thank you very much. That concludes the questioning.

Every Senator who left told me this has been a really great hearing. The members of the panel are deeply appreciated. We did not even get to get as deep as any of us wanted to on a lot of what you wanted to say and what we wanted to discuss with you, but that will come, and we do have consensus that we need to move and move broadly and quickly, but effectively.

And your testimony today and what you will continue to give us in terms of counsel and advice and response to questions will help us get that done.

So, again, thank you all very much. You will probably get some more questions from Senators, and to those Senators who wish to submit questions for the record, those are due to the Committee by Thursday, October 31st. And then we ask that you respond to them as quickly as you can when you do receive them.

With that, again, thank you very much for being here, and this Committee is adjourned.

Mr. RITTER. Thank you, Mr. Chairman.

Mr. MARLOW. Thank you, Chairman.

[Whereupon, at 11:29 a.m., the hearing was adjourned.]

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

PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

We welcome to the Committee four witnesses with extensive experience and a range of perspectives on issues related to data ownership, valuation and privacy, including: Mr. Jeffrey Ritter, Founding Chair of the American Bar Association Committee on Cyberspace Law, and an external lecturer at the University of Oxford; Mr. Chad Marlow, Senior Advocacy and Policy Counsel at the American Civil Liberties Union; Mr. Will Rinehart, Director of Technology and Innovation Policy at the American Action Forum; and Ms. Michelle Dennedy, Chief Executive Officer of DrumWave.

As a result of an increasingly digital economy, more personal information is available to companies than ever before.

Private companies are collecting, processing, analyzing and sharing considerable data on individuals for all kinds of purposes.

There have been many questions about what personal data is being collected, how it is being collected, with whom it is being shared and how it is being used, including in ways that affect individuals' financial lives.

Given the vast amount of personal information flowing through the economy, individuals need real control over their personal data.

This Committee has held a series of data privacy hearings exploring possible frameworks for facilitating privacy rights to consumers.

Nearly all have included references to data as a new currency or commodity.

The next question, then, is who owns it? There has been much debate about the concept of data ownership, the monetary value of personal information and its potential role in data privacy.

Some have argued that privacy and control over information could benefit from applying an explicit property right to personal data, similar to owning a home or protecting intellectual property.

Others contend the very nature of data is different from that of other tangible assets or goods.

Still, it is difficult to ignore the concept of data ownership that appears in existing data privacy frameworks.

For example, the European Union's General Data Protection Regulation, or GDPR, grants an individual the right to request and access personally identifiable information that has been collected about them.

There is an inherent element of ownership in each of these rights, and it is necessary to address some of the difficulties of ownership when certain rights are exercised, such as whether information could pertain to more than one individual, or if individual ownership applies in the concept of derived data.

Associated with concepts about data ownership or control is the value of personal data being used in the marketplace, and the opportunities for individuals to benefit from its use.

Senators Kennedy and Warner have both led on these issues, with Senator Kennedy introducing legislation that would grant an explicit property right over personal data, and Senator Warner introducing legislation that would give consumers more information about the value of their personal data and how it is being used in the economy.

As the Banking Committee continues exploring ways to give individuals real control over their data, it is important to learn more about what relationship exists between true data ownership and individuals' degree of control over their personal information; how a property right would work for different types of personal information; how data ownership interacts with existing privacy laws, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and GDPR; and different ways that companies use personal data, how personal data could be reliably valued and what that means for privacy.

I appreciate today's witnesses for offering their expertise and sharing a range of unique perspectives.

PREPARED STATEMENT OF SENATOR SHERROD BROWN

Thank you to the Chairman for calling this hearing.

This Committee has spent some time over the last several months discussing Facebook's poorly thought out plan to create a global currency. And the bottom line is that we know that Facebook can't be trusted with Americans' personal information and it is terrible at protecting its users' privacy. It was pretty clear the last thing we should do is trust them with American's hard earned dollars.

But it isn't just Facebook. Every time corporations in Silicon Valley come up with a new business model, the result is the same—they get more access to our personal

data, spending habits, location, the websites we visit, and it means more money in their pockets. And everyone else gets hurt.

So I want to begin this hearing with a simple question—who has the right to control your personal, private information: you or Silicon Valley CEOs like Mark Zuckerberg?

I think we all agree that Americans should have more control over their private information.

But should we treat that private information like property? Today's witnesses will discuss that idea.

At first glance this might seem like a simple way to tackle the complex problems created by data collection and machine learning.

The promise is that if we just treat personal data like property, markets will do the hard work of protecting our privacy for us.

But that's not how it will work.

Instead of making companies responsible for protecting their customers' privacy, this idea puts the burden on all of us.

Now imagine that if every time you wanted to use Facebook, or pay for something with an app, or login to a Wi-Fi network, you had to read even more legal fine print, and check a box saying, "OK, I waive my personal right to my data to use this service." Or you had to join some kind of so-called "data collective" to sell your data.

Working people in this country have enough to worry about—they're trying to get the kids out the door and get to work on time; to make rent and save for college and pay the bills.

The idea that people should also have to manage their data like a landlord manages its tenants is ludicrous.

This should be pretty simple—corporations should not be allowed to invade our privacy.

We know that today, they are.

Just think about all the personal data that's already floating around out there. Equifax exposed the personal information of more than 150 million Americans—Social Security numbers, birthdays, addresses. Capital One exposed the personal information of more than 100 million Americans.

How can you own your data, when it's already littered all over the internet?

Big tech companies don't want to protect your personal information—they want to profit off it. Protecting your privacy doesn't make them any money—it costs them money—so they aren't going to do it.

They want your data, and they want to get it for free, or pay as little as possible for it.

So it should be no surprise that I am skeptical when I hear of plans for Americans' data to be treated like property.

If Americans want more control over their private information, we have to find a way to prevent corporations from mining our data and selling it to each other. Creating a supermarket for selling away our privacy does the opposite.

Treating data as something that can be owned, bought, and sold doesn't solve any of these problems—especially when undermining our privacy is the business model.

Mark Zuckerberg and his Silicon Valley buddies want us to skip over the part where we have control over our privacy, and jump to the part where giant tech companies get to use their market power to squeeze our privacy out of us—and it would all be legal.

That's unacceptable.

I appreciate that Chairman Crapo has been working with me in a bipartisan way to create real privacy protections. Privacy isn't partisan, it's a basic right.

I look forward to continuing our work together, and to the witnesses' testimony.

Thank you.

Statement of Jeffrey Ritter

Founding Chair of the American Bar Association Committee on Cyberspace Law; External Lecturer at University of Oxford, Department of Computer Science (on research sabbatical)

United States Senate
Committee on Banking, Housing, and Urban Affairs
October 24, 2019
Hearing on "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation"

Good morning Chairman Crapo, Ranking Member Brown, and members of the Committee. Thank you for the opportunity to join you, speaking in my role as an active contributor for over 30 years to law reforms enabling US and global electronic commerce. The time is long overdue for comprehensive privacy reform legislation. For now, we just seem to have been relegated to playing 'catch-up' with the EU and other nations that have embraced their rules; we are trying merely to weave together our piecemeal laws into some type of whole cloth.

Privacy law reform here will surely fail if we do not incorporate something new—a legal answer to the most fundamental question: who owns digital information? For the totality of digital information, this is an enormous chasm in the evolution of the rule of law for the Digital Age. For personally identifiable information, the question is particularly relevant. Yes, it is identifiable, but who owns it?

In many steps to advance electronic commerce, the United States has led the world, notably enabling electronic contracts and electronic signatures to be legally valid without paper. Indeed, in humankind's history, no rule of law was more rapidly incorporated into the laws of the world than the rules we helped innovate to enable digital commerce to become real. But, in privacy, we are behind.

To re-establish this nation's leadership, privacy reform must express clear, explicit rules that establish who owns any specific digital file or record. Only then can we be successful in crafting the additional rules for

acquiring, using, transferring, selling, and controlling personal data, and imposing the sanctions for violating those rules.

Think about it. Every commercial system built on the rule of law—real estate, banking, consumer and industrial products, mining—begins with a commitment to define and protect the rights of the owner of the property. Yet, across all privacy law, while a data subject has many controls on the use of identifiable information, and we often speak in conversation about ownership, the legal right of ownership has not been established.

As summarized in a recent article submitted as part of my written testimony, Germany, Japan, and the OECD are all calling for formal legal rules on data ownership, including from Chancellor Merkel herself. Japan has already published model guidelines for structuring data sharing and licensing agreements based on ownership principles. Failing to address data ownership in our privacy reforms will surely further isolate the United States from the global momentum and allow the rules for data as property to be written by others.

The solutions on how to craft this legal concept are already part of Federal law, within the laws governing electronic transferable records[1] and, at the global level, in recently finalized UN model laws[2] authored with substantial US input and influence. There, the rights of ownership are exercised by establishing and maintaining "control" over the digital file. Realistically, the first owner of personal data will be the business entity with which a data subject is engaged—a bank, a broker, a hospital, a university. Their systems create the control over the personal data. But recognizing data ownership should do nothing to remove or

---

1 15 U.S. Code §7021. Transferable Records. The statute enables a person "in control" of a qualifying electronic transferable record to act as a *holder* under the Uniform Commercial Code, able to exercise the rights and defenses of a holder in due course or purchaser (i.e., acting as the owner of that record).

[2] UNCITRAL Model Law on Electronic Transferable Records (2017), available at https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records.

diminish a data subject's rights and controls—indeed, if ownership is clear, accountability for violating those controls can be more readily enforced. As more fully explained in my written testimony, writing these rules should not disrupt any of our existing Federal laws for protecting personal information, including those governing our financial systems.

As to valuation, there is an essential truth: The accurate valuation of any asset in commerce begins with a calculation of the certainty of ownership. Any calculation of the economic value of personal information will be inherently inaccurate if ownership and the related rights are not certain. The new California privacy law has attempted to address valuation but its silence on ownership fatally handicaps that effort.

Privacy law reform to merely play catch-up with the EU will not be enough. To seize the opportunity, the US must address and define ownership rights in personal information. This will move the US ahead in providing a more stable, predictable legal environment in which the value of personal information can be more fairly calculated, the rights of data subjects more readily enforced, and commercial innovation built around personal information can thrive.

I will defer to my submitted written testimony for my responses on other topics the Committee invited me to address. Thank you.

***

Supporting Additional Testimony

In support of my oral testimony today, the following is offered to expand upon several of the topics introduced and to provide further substantive material for the Committee.

Background Perspective

Since 1988, I have been actively engaged in identifying legal barriers to electronic commercial practices, eliminating those barriers, and crafting the rules that would enable the legal validity and expansion of those practices. Most notable was my work as the founding chair of the American Bar Association, Section of Business Law, Committee on Cyberspace Law and my active service, on behalf of the United States, in the United Nations' varied programs that produced a foundation for global digital trade.

At the UN, I served as a co-rapporteur on legal questions for the UN Economic Commission for Europe Working Party on the Facilitation of International Trade Procedures.[3] In that role, I led efforts that ultimately involved more than 80 nations and non-governmental nations in formulating legal solutions to advance electronic commerce. I also participated extensively in the activities of the United Nations Commission on International Trade Law (UNCITRAL)[4] and the United Nations Conference on Trade and Development (UNCTAD)[5], and, in 1997, had the opportunity to contribute to "A Framework for Global Electronic Commerce" strategic plan of the United States.[6]

"Electronic information—data—is emerging worldwide as a fundamentally new species of property. Data is being created, manipulated, stolen, bought, sold, leased, stored and transported in transactions for which our existing laws . . . no longer provide easy accommodation." This statement was published in July 1993 as part of the Mission Statement for The DataLaw Report, for which I served as co-founder and editor-in-chief (copy attached as Annex A). The first issue's lead article addressed privacy rights of employees in the workplace. Even earlier, beginning in 1989, through my UN work, I actively interacted with EU representatives on privacy issues, for which they lobbied to align international work products with the EU's privacy laws.

In the last decade, I have continued to engage on these topics, crafting at Johns Hopkins University, Whiting School of Engineering a graduate course on "Privacy Engineering", as well as teaching at the University of Oxford, Department of Computer Science a course titled "Building Information Governance." My most recent book, Achieving Digital Trust: The New Rules for Business at the Speed of Light, was used as the text for that course and has been adopted at other universities. A full c.v. has been previously submitted to the Committee staff.

Regulating Data as Property: A New Construct for Moving Forward

In late 2018, the Duke Law & Technology Review published an article I co-authored with a research assistant, Anna Mayer, "Regulating Data as Property: A New Construct for Moving Forward" (copy attached as Annex B)[7]. While the analysis focuses on personal information and privacy law, the overall scope is broader and introduces a new classification scheme to better enable incorporating ownership rights into the larger legal structures already in existence (see A New Concept for Classifying Digital Information below).

The article presents in substantial detail the following elements referenced in my oral statement:

- The policy statements of Germany, Japan (through METI), and the OECD on data ownership as a key priority for enabling innovation in commerce.

[3] The work products of that group are now incorporated into the work of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). See https://www.unece.org/cefact.html.
[4] Key work products of UNCITRAL that were produced or initiated during the tenure of my work included the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures, each of which are available at https://uncitral.un.org/en/texts/ecommerce.
[5] In addition to authoring for UNCTAD a special report on the legal facilitation of electronic commerce for developing nations, I had the privilege of helping secure and host in Columbus, Ohio a meeting of the United Nations which produced the Columbus Ministerial Declaration on Trade Efficiency, available at http://sunsite.icm.edu.pl/untpdc/tei/columbus.html.
[6] Available at https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.
[7] 16 Duke Law & Technology Review 220-277 (2018), available at https://scholarship.law.duke.edu/vol16/iss1/7.

- A summary of international privacy law, to the extent available to us in the English language (or translations), notably the conclusion that no formal law addresses ownership of personally identifiable information.
- The relevant provisions of the Uniform Commercial Code and Federal law, as well as the United Nation work product, that serve as a model for how to structure the definition of ownership and adapt concepts of "control" toward creating the legal formalities for defining the ownership of data.

Our analysis also examined several additional points of possible interest to the Committee:

- Recognition that, as a matter of consensus in the scientific community, information (including digitally recorded information) is best considered as a physical asset, rather than treatment as an "intangible" thing.
- An analysis of how US Copyright law and the EU Database Directive have failed to deal with digital information ownership rights, and their inadequacy in doing so.
- A survey of the advocacy relating to the automotive industry (outside the United States) calling for clear, certain rules for data ownership.

A New Concept for Classifying Digital Information

The current portfolio of laws protecting information is awkwardly suited to enabling better expressions of ownership rights in digital information. For too long, we have tried to "fit" the realities and trends of digital commerce into legal structures that were written before computers and the Digital Age were considered. Notably, both in the US and the EU, adjustments to copyright law have been ineffective and inconsistent. The article offers a new classification scheme:

- Factual Data, which can be either
    - Personal Information (or Personally Identifiable Information), or
    - Industrial Data (everything else that is factual)
- Fictional Data.

This scheme enables the following immediate benefits to advancing data ownership principles:

- By separating Factual Data from Fictional Data, copyright laws (which were intended to protect Fictional Data) can be revised, providing more robust and focused protection for both classes.
- Personal Information can itself be given appropriate rulesets which enable both ownership and data subject rights and controls.
- Industrial Data can also be given dedicated, appropriate rulesets that address ownership, and also better advance the data sharing, data analytics, distributed systems, and other innovations which exist and will continue to evolve.

Who is the First Owner of Personal Information?

As mentioned in my oral statement, a data subject is *not* likely to be the first owner of personal information identifiable to that individual. Yes, the data is personal, possibly intensely personal, but the primary reason a record of that information is being created is to enable effective transactions between the individual and another entity—a retail store, a hospital providing medical care, a financial institution servicing an account, a broker managing investments, an airline transporting passengers or shipments.

Any of those entities are investing enormous amounts in their systems to gather, store, analyze and use the data to deliver the primary services. Legitimately, as the data creators, they have always felt they "owned" the data, and the emergence of privacy concerns was not driven by their entitled sense of ownership but by another far more substantive force.

What commerce, industry, and governments as a whole did not appreciate, as those systems were being developed, were the powerful, dynamic manners in which any data, once gathered, could find secondary uses and secondary, downstream markets, when aggregated, analyzed, parsed, and combined with other data sources. As networking, data standards, high-speed communications, and computational power have evolved, new ways were created in which data, once shared, could transform a company's revenue, productivity, and quality of services.

These capabilities are what shifted the momentum of concern regarding privacy—once data began to be a functional commodity to be shared, the privacy of the data subject became vulnerable. Yet, while the last 30 years have seen evolutions in the rights of a data subject to control those sharings and uses, the issue of ownership has never been formalized into any legal structure.

It is my view that the original point of recordation of information—whether on a phone, a device, or a server—is the starting point where ownership can be asserted, through the exercise of "control" as more expansively explained in the article (Annex B). For personal information, this is also where the negotiation between a data subject and the owner regarding how the personal data can be used (and the rules and controls required) is best placed.

Here is an example:

> A new automobile in 2019 is basically a data collection tool also operating to provide transportation. Within the machine, there are dozens of sensors that not only monitor geographic location, speed, and operator behavior, but also continually measure and report on performance of the functional components. Unless the driver has uniquely 'logged in' with a unique ID (such as a biometric sensor panel), the vehicle knows nothing about the identity of the actual driver (i.e., it is Industrial Data). Yet all of that data is intensely valuable to the manufacturer, component suppliers, public authorities managing traffic flow patterns, and many others.

But who owns the data as the vehicle drives off a dealer's lot? The component suppliers? The software developer whose software is installed in those components? The manufacturer? The captive leasing company that has leased the vehicle to a new driver? Perhaps the driver has elected to retain the data all to themselves! Indeed, going forward, in an Internet of Things (IoT)world, virtually every product is two things: a service provider and a data collection and communication device. *Nearly ubiquitous surveillance is advancing; who owns the data streams?*

It is easy to imagine that the dealer may offer the driver two prices: one price is for a vehicle with no data-sharing services; the second, at a lower price (taking account of the downstream economic value of the data), allows the data sharing. A third, at an even lower price, may be tied to matching the Industrial Data to related Personal Data (such as the identity of individual drivers) and, in that instance, negotiating the controls on secondary, downstream transfers and uses of the personal data.

Today, however, many consumer IoT devices offer no such negotiation and the existing privacy laws do nothing to produce meaningful descriptions of the transactions (and revenues) the device manufacturer

realizes under the "consent" given by the purchaser. But the manufacturer, in nearly every instance, is acting as the de facto owner of the collected data.

Why not provide legal certainty to that situation? Doing so makes the negotiation of the rights and controls far easier to accomplish. The economic valuation of the data can be more easily incorporated into the negotiation—perhaps even as a separate item for which different data subjects may be induced to pay greater or less value for the device itself.

Data Ownership and Existing Federal Laws (Privacy in Financial Systems)

Data ownership must be addressed at a global level, allowing concise, known rules for determining who owns a specific data asset to be understood and applied irrespective of the geographic location of the participants. We have achieved that certainty for physical goods[8]; doing so for digital information is imperative. Ideally, the law reforms required would address both Industrial Data and Personal Data, as well as include adjustments to copyright laws where the distinctions between Fictional Data and Factual Data have been muddled by previous enactments (such as the Digital Millennium Copyright Act).

But a useful and constructive step in the right direction is to establish a doctrine of ownership for personal information. As part of the privacy reform this nation is contemplating, it is critical that we abandon industry-specific sectoral solutions (like Gramm-Leach-Bliley Act, Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act) and embrace an omnibus model similar to the EU's GDPR and related rules and regulations. In doing so, substantial alignments must be made, but adding data ownership rules into that alignment process should do little to disrupt the reforms of existing rules in order to be responsive to the greater expressions of rights and controls sought be data subjects.

Data Ownership and California Privacy Law

While privacy advocates may applaud the new rules in California[9], defaulting to the enactment of privacy law reforms by individual states is in fundamental conflict with the trends and practices of international, global commerce, as well as the integrity and fluidity of interstate commerce in the United States. Privacy is a topic on which uniformity is incredibly important; that demand is one reason why the GDPR rules from the European Union have been so readily adopted more broadly across global trade. It is simply the nature of computing to seek uniform, standardized rules.[10]

As briefly noted in my oral statement, the California law does take an affirmative step toward improving the economic valuation of data, and moving calculations of value into the transactions between a data subject and data collector.[11] But the law is silent on ownership. Having not been involved in the drafting or negotiation of the CCPA, I have no insight into that outcome. It is an opportunity missed, though I strongly believe a uniform Federal solution is to be preferred.

---

[8] *See* The United Nations Convention on Contracts for the International Sale of Goods, available at https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf.

[9] California Consumer Privacy Act of 2018, Cal. Civ. Code Section 1798.100-1798.199) ('CCPA').

[10] In turn, these influence our business practices. For example, the invitation from the Committee for my testimony instructed that this testimony be submitted in a single format-Microsoft Word.

[11] See Cal. Civ. Code Section 1798.125(b) and Article 6 of the Proposed Regulations, available at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

Data Ownership and Data Valuation

The accurate valuation of any asset in commerce begins with a calculation of the certainty of ownership. When there is uncertainty as to ownership, any negotiated value will be lower. Yet, for personal data, the absence of any defined mechanism for establishing ownership inherently reduces valuation, and makes any calculation of value difficult to execute with any accuracy.

There can be little disagreement that the vast collections of digital personal data already built during the last 40 years have been collected with no explicit awareness of ownership nor valuation, at least at the point of collection. In the downstream, secondary marketplace in which personal data is the asset of the transactions, various valuation mechanisms have developed. However, none of them are particularly effective because, since ownership cannot be legally verified, all transaction participants carry some risks.

Those risks have several adverse impacts on the transactions. First, the valuations are going to be less, discounted by some economic expression of the value of those risks. Second, the transaction costs, particularly legal fees (and time) incurred to negotiate how the risks will be allocated, degrade the net present value of the transactions to the participants—even if the controlling party has strong confidence that the proposed use of the personal data in the transaction has been approved by the privacy consents of the related data subjects.

I have no particular competence to offer an opinion on the valuation methods to be used with personal data. But I do know that certainty of ownership will contribute to improved certainty in valuations, as well as eliminate risks, accelerate transaction velocity, and provide a substantive foundation for continued innovation in the use of personal information in the marketplace.

Personally, while I want to know what data is collected about me, I have few objections to a world in which our systems and devices do so. The results are more personalized, focused interactions: A hospital can more immediately, and accurately, deliver medical care; a financial institution can tailor cross-marketing more effectively and better protect my financial assets; and advertising, whether as online banners or in direct marketing, is more focused to my interests and needs.

Personal data has become a new kind of asset for which, as a data subject, I want to have controls on its use and be more fairly compensated for the value that data provides to the collecting entity with which I am engaging. Understanding who owns that data will make those transactions more functional and useful across our economy and our global systems.

Data Ownership and Digital Trust

Writ large, privacy law serves to secure the trust of data subjects with the collection and use of their personally identifiable information. As discussed at length in my most recent book, Achieving Digital Trust, trust is not an emotion, but the result of complex calculations in which we identify the rules we expect to govern particular transactions and evaluate the quality with which those rules are executed. When suitable rules do not exist, or existing rules are not executed, our determinations to trust are impaired or, in the worst case, impossible to calculate.

For privacy, the rules and regulations expressed in formal public law are the first step; however, effective execution of those rules requires policies, procedures, terms of use, and contractual agreements to be

authored, implemented, and capable of enforcement, whether by the transaction participants, self-regulatory organizations, or public authorities.

In addition, all of those rules must be mapped into software code and applications, capable of being executed automatically and also capable of keeping logs of their due execution to provide adequate proof of compliance with all of the rules. Collectively, there are a lot of rules, and each rule is an opportunity for risk when that rule is ignored, not properly implemented, or not supported by proper records of the due execution of those rules.

The inventory of the rules for privacy, on a global level, is complex. Billions of dollars are spent trying to build systems and processes that are in compliance.[12] The situation is the more difficult when an organization's operations or customer assets cross multiple boundaries and thereby invoke different rules applicable to defined subsets of information. This is another functional reason why companies rightfully should seek a Federal solution versus state-by-state privacy reforms.

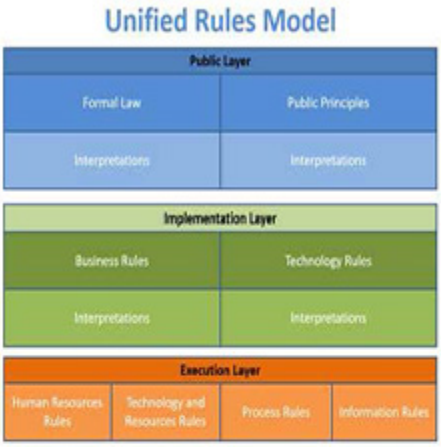
"Privacy by design" is an important concept. In its essence, it advocates creating a full inventory of the applicable rules *before* responsive systems and processes are constructed, thereby dramatically improving the probability all of those rules are being satisfied. The result is intended to be greater trust, calculated because of the knowledge that a specific system has been well-designed to the rules.

The metaphor to a residential home or commercial building is easy to imagine—who could build any such structure without first accounting for, and providing evidence of compliance to the relevant building authority prior to occupancy for, all of the building code rules?

I believe the key principles of rules-based design should not be limited merely to systems managing or interacting with personal data; the principles should be expanded to all systems. I similarly advocate that data ownership should be clear with respect to all types of data. But the overall task of organizing and assembling those rules into a unified, coherent inventory will be challenging. Moreover, different governance models (i.e., common law, civil law, authoritarian law) strike different balances among the various rule types, particularly with regard to how much flexibility private sector actors have in authoring the non-public rules (policies, procedures, terms of use, privacy notices, etc.) that still must be present for trusted services to be delivered.

To provide structure to these tasks, one tool that may be helpful as the Committee analyzes how to proceed, is the Unified Rules Model—a visual tool for classifying and organizing the rules required to engineer improved compliance and governance of any system, application, or device.

[12] A new report prepared for the California state attorney general by an independent economic research firm projects initial compliance costs with the new CCPA may be as much as $55 billion. https://www.cpomagazine.com/data-protection/new-report-suggests-initial-compliance-costs-for-ccpa-could-reach-55-billion/.



The detailed classifications and uses of the Unified Rules Model are described in detail in Achieving Digital Trust (a hard copy of which has been provided as Annex C to Committee staff in support of this written testimony).

****

Please feel free to contact me with any further questions relating to my testimony at jeffrey@jeffreyritter.com, jeffreyritter54@gmail.com, or 202.285.7385.

The DataLaw Report

Analyzing the changing global legal environment for electronic information

Vol. 1, No. 1 July 1993

Employers' Access To Employee E-Mail

E-Mail Privacy Versus Corporate Privilege

More and more companies are implementing electronic mail systems to improve and expedite internal and external communications. E-mail is beginning to rival the telephone as a means of conducting business: organizations implementing E-mail find that it "flattens the management hierarchy, improves project tracking, and speeds time to market for new products or services." A. Reinhardt, *Smarter E-Mail is Coming*, BYTE vol. 18, no. 3, p. 90 (March 1993). One estimate is that the number of LAN E-mail users in the United States rose 60 percent last year, will climb another 60 percent this year to 15.1 million users, and will be up to 38 million in 1995. Meanwhile, the number of messages transmitted within Fortune 2000 firms in North America will surge from 6.1 billion in 1993 to 14.3 billion in 1995. Id., citing research by the Yankee Group (Boston, Mass.), and the Electronic Mail Association (Arlington, Va.).

The increased use of electronic mail in commercial practice has led to increased concerns about the privacy rights of the users of such systems, and the rights of employers to gain access to E-mail transmissions. Several recent controversies have highlighted the dilemmas facing employers and employees when electronic messaging technologies are used.

In 1992 a software vendor, Borland International, Inc., found E-mail evidence that a former employee, Eugene Wang, had transmitted confidential business information to a rival company, Symantec Corp., via

(Continued on page 7)

IN THIS ISSUE:

Published by CLARK BOARDMAN CALLAGHAN • 155 Pfingsten Road • Deerfield, Illinois 60015

The Negligent Operation of Electronic Networks

Judicial Standards of Accountability

The movement of information has always been an essential aspect of commerce. Information must be communicated in the course of every commercial transaction. With the advancement of technology, the ability to send and receive information electronically has created the opportunity for companies to increase their portfolio of activities to include the business of sending and receiving information, both for themselves and as a service provider to third parties. Initially with electronic mail, and now with electronic data interchange (EDI), the business of sending, receiving, storing and processing information in the course of conducting business has become a separate and viable enterprise, introducing into commerce a new class of commercial player—the value-added network or VAN.

The Role of Value-Added Networks

There is no question that networks have become indispensable to the current and foreseeable expansion of electronic commerce. Much as we have developed an integrated, multi-modal, global network for the physical transport of goods, so have the individual networks become the essential components of an integrated framework for the advancement of electronic commerce. Even with the exist-

(Continued on page 11)

The DataLaw Report Mission Statement

The DataLaw Report exists to provide a means for reporting upon and analyzing the changing global legal environment for electronic information. Electronic information—data—is emerging worldwide as a fundamentally new species of property. Data is being created, manipulated, stolen, bought, sold, leased, stored and transported in transactions for which our existing laws, set forth in the diverse legal systems of an emerging global economy, no longer provide easy accommodation. Electronic information has become something deserving of its own rules, and it is now apparent that the law will be responsive.

By giving focus to both new and divergent areas of law, **The DataLaw Report** will become an essential tool for enabling companies, their attorneys and other information professionals to learn and master the new rules of the game.

Korea Requires Electronic Commerce

New Law Requires EDI for International Trade Documents

There remains little question that implementing EDI yields competitive advantage for those first to recognize its potential for efficiency, accuracy and speed. Korea has become the first nation to promote the automation of the exchange of commercial and administrative documents through national legislation, the Act on Promotion of Trade Business Automation (Law No. 4479, Dec. 31, 1991). The legislation is a revealing work, demonstrating unequivocally the prospects for further national policy-making by other countries and regions.

The Ministry of Trade and Industry (MTI) promoted the Act in order to accelerate the establishment of a paperless trading system. According to documents in English provided to the United Nations by the Korea EDIFACT Center, the goal is to establish the ability of trading companies and trade-related administrative bodies to electronically exchange information normally moved by traditional paper documents. The scope of the Act is impressive; MTI includes on its agenda trade administration, customs, banking, insurance and transport activities. It is hoped that pursuit of automation in these areas will improve the competitiveness of local trading companies in the international

(Continued on page 14)

REGULATING DATA AS PROPERTY: A NEW CONSTRUCT FOR MOVING FORWARD

JEFFREY RITTER AND ANNA MAYER †

ABSTRACT

The global community urgently needs precise, clear rules that define ownership of data and express the attendant rights to license, transfer, use, modify, and destroy digital information assets. In response, this article proposes a new approach for regulating data as an entirely new class of property.

Recently, European and Asian public officials and industries have called for data ownership principles to be developed, above and beyond current privacy and data protection laws. In addition, official policy guidances and legal proposals have been published that offer to accelerate realization of a property rights structure for digital information. But how can ownership of digital information be achieved? How can those rights be transferred and enforced?

Those calls for data ownership emphasize the impact of ownership on the automotive industry and the vast quantities of operational data which smart automobiles and self-driving vehicles will produce. We looked at how, if at all, the issue was being considered in consumer-facing statements addressing the data being collected by their vehicles.

To formulate our proposal, we also considered continued advances in scientific research, quantum mechanics, and quantum computing which confirm that information in any digital or electronic medium is, and always has been, physical, tangible matter. Yet, to date, data regulation has sought to adapt legal constructs for "intangible" intellectual property or to express a series of permissions and constraints tied to specific classifications of data (such as personally identifiable information).

---

† Jeffrey Ritter, J.D. is a Visiting Fellow at Kellogg College, University of Oxford, where he is researching and writing on the first principles of quantum law. He is an External Lecturer at Oxford, teaching in the Department of Computer Science, and also teaches Privacy Engineering at Johns Hopkins University, Whiting School of Engineering. Anna Mayer is a graduate student at the Institute of Political Science, University of Vienna, M.A. expected 2018. Anna Mayer is researching the concept of e-residency at the Ragnar Nurkse Institute of Governance and Innovation, Technical University Tallinn. A preliminary draft of this article was presented at MyData2017 in Tallinn, Estonia on August 30, 2017 and the additional input and comments from Triin Siil are greatly appreciated.

We examined legal reforms that were recently approved by the United Nations Commission on International Trade Law to enable transactions involving electronic transferable records, as well as prior reforms adopted in the United States Uniform Commercial Code and Federal law to enable similar transactions involving digital records that were, historically, physical assets (such as promissory notes or chattel paper).

Finally, we surveyed prior academic scholarship in the U.S. and Europe to determine if the physical attributes of digital data had been previously considered in the vigorous debates on how to regulate personal information or the extent, if at all, that the solutions developed for transferable records had been considered for larger classes of digital assets.

Based on the preceding, we propose that regulation of digital information assets, and clear concepts of ownership, can be built on existing legal constructs that have enabled electronic commercial practices. We propose a property rules construct that clearly defines a right to own digital information arises upon creation (whether by keystroke or machine), and suggest when and how that right attaches to specific data though the exercise of technological controls.

This construct will enable faster, better adaptations of new rules for the ever-evolving portfolio of data assets being created around the world. This approach will also create more predictable, scalable, and extensible mechanisms for regulating data and is consistent with, and may improve the exercise and enforcement of, rights regarding personal information. We conclude by highlighting existing technologies and their potential to support this construct and begin an inventory of the steps necessary to further proceed with this process.

INTRODUCTION

The rapid and accelerating development of data analytics, automated manufacturing, probability-based management practices, machine-based commodities trading, and other innovations is generating an entirely new global awareness of the economic value and functional utility of digital information. All of these industrial creations confirm that data has now become a new kind of property—an asset that is created, manufactured, processed, stored, transferred, licensed, sold, and stolen. Yet, on a global basis, there is no legal regulatory framework or model that

provides guidance on how transactions using data as an asset are to be constructed.[1] That void in the rule of law can no longer be overlooked.

Reforms in copyright law to address digital creative works and the continuing evolution of regulations for personal information are important. But these adaptations to the realities of our digital world are not sufficient; indeed, there is little question that the largest volumes of digital information that already exist, and continue to be created, have two distinctive features which make copyright and privacy law adaptations inadequate. First, these enormous data sets have nothing to do with the creative artistic assets that copyright laws serve to protect. The data are industrial in nature, generated by vast networks of sensors that observe and record the smallest units of entire global supply chains. Second, they have nothing to do with personally identifiable information. The data are functional to how machines, networks, systems, devices, and information interact with one another and perform against their defined objectives. Something more is needed, urgently.

In recent months, both in Europe and in Asia, public officials and industry organizations have been declaring a need for the ownership of data to be explicit and confirmed by legal instruments.[2] Once ownership is well-defined, then the attendant rights can be more precisely expressed—rights to access, license, transfer, modify, combine, edit, and delete data naturally flow from the control that ownership vests.[3] In addition, both existing and new types of transactions can be more formally expressed (e.g., licenses, sales, transfers, processing services, storage services, analytics, and more).

There is no question that these types of transactions are occurring already. The Worldwide Semiannual Big Data and Analytics Spending

---

[1] Electronic commercial practices have frequently faced legal hurdles as each new generation of technology places stress on the state of the rule of law that then exists. Model agreements and model laws, when developed and published, offer solutions on how those hurdles can be overcome. *See, e.g.*, MODEL FORM OF ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT AND COMMENTARY (Am. Bar Assoc., 1989); *Model Contracts for the Transfer of Personal Data to Third Countries*, EUR. COMM'N, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last visited Nov. 7, 2017); *Sample Business Associate Agreement Provisions*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (last visited Nov. 7, 2017) (providing samples for health information privacy); INTERMODAL INTERCHANGE EXEC. COMM., UNIFORM INTERMODAL INTERCHANGE AND FACILITIES ACCESS AGREEMENT (2018), *available at* http://uiia.org/assets/documents/newuiia-Home.pdf (providing samples for, among other items, electronic and non-electronic receipts for equipment interchange).

[2] *See infra* Part II.

[3] *See infra* Part V.

Guide from International Data Corporation estimates that big data and business analytics alone will create US$203 billion in annual revenues by 2020, with revenue growth from information-based products (data monetization) doubled by the end of 2017 for one third of the Fortune 500 companies.[4] But who owns the assets that are the focus of these deals?

This article offers a bold proposition: An explicit, legal mechanism to establish, claim and transfer property rights in data must be adopted. Doing so rapidly is essential to enable digital commerce to evolve while continuing to assure the enforcement of privacy and data protection rules and existing intellectual property law constructs.

The critical insight on which this proposition rests is the scientific consensus that digital information is not intangible, but is physical, tangible matter. Governance of data, including personal information, will best be achieved by leveraging existing legal systems that govern the ownership, use, and transactions of the other physical assets which are the assets of economies, commerce and wealth.

Sales transactions, licensing deals, joint ventures, downstream distributions and syndications of rights to access and use data, valuation for accounting and tax purposes—all of these are possible, and some are already occurring. But defining ownership to attach to physical data will provide the proper foundation on which the globalization and continued growth of digital markets can proceed. To fail to do so, and to continue to focus only on the regulation of personal information without addressing the critical need to define and enable ownership of *all* data, renders a major disservice to the potential of the Digital Age in which we now live to be achieved.

This paper proceeds as follows. First, to facilitate our analysis, Part I introduces and defines certain terms useful to analyzing data ownership. These terms present important elements for how to discuss the totality of digital information, beyond the boundaries of personal information that current public regulations emphasize. Part II reviews current policy statements supporting the call for data ownership, as well as proposed legal reforms and innovations in business practices involving the automotive industry in Europe and Asia. A summary of the current state of the law for industrial data also is presented, to highlight that clear principles of ownership for all types of data have not yet been adopted. In Part III, existing academic literature on the suitability of property rights systems for data is surveyed and two additional essential conclusions are presented.

---

[4] Gil Press, *6 Predictions for the $203 Billion Big Data Analytics Market*, FORBES (Jan. 20, 2017, 9:27 AM), https://www.forbes.com/sites/gilpress/2017/01/20/6-predictions-for-the-203-billion-big-data-analytics-market/#498daf472083.

Part IV introduces the scientific literature regarding the physical quality of information, which supports the essential conclusion that data is physical, tangible matter, no different in its essential attributes than any other physical property (for which humankind has developed robust, mature, and functional property right systems, such as those governing real property, commodities, or manufactured goods).

The paper concludes in Part V with our proposal on how to proceed forward to install a property rights legal foundation for data that can work globally and be scalable across the diversities of existing and future systems, nations, and data classifications. The proposal builds on the physical nature of digital information and leverages the model law that has recently been adopted at the United Nations for transferring control of electronic records with legal value, as well as predicate constructs adopted in the U.S. Uniform Commercial Code and Federal law. Additional next steps for moving the proposal forward into contractual and regulatory legal systems are suggested.

I. DEFINED TERMS

For the purposes of this article, the following terms will be used. These terms have been developed in order to facilitate the discussion presented. The definitions are not scientifically precise; rather, they are intended to focus the analysis and, hopefully, enable ongoing dialogue about the utility and application of a property rights legal foundation for data.

> *Data* means any information recorded by electronic or digital means and is retrievable, whether perceivable to a human or machine.[5]
>
> *Industrial data* means any data that is created, processed, stored, or used in commerce, including business-to-business transactions, and excludes any personal information. Manufacturing, production, transport, mining, shipping, aeronautical traffic, financial services, securities markets—these are representative examples of the sources and uses of industrial data.
>
> *Personal information* (or personally identifiable information, or "PII") means any information that may be identified with a data subject or individual person, whether or not formally defined as such by any applicable statute, regulation or other legal requirement. For our purposes, personal information includes, but is not limited to,

[5] *See infra* Part IV. This definition is an adaptation of the definition of "record" introduced into the Uniform Commercial Code to provide a technology-neutral word that would include both paper-based and digital information records. The adaptation adds including information that is perceivable by a machine, but which may not be sensible to humans.

"personally identifiable information" as such term--and similar terms--are defined in various statutes and public laws.[6]

Factual Data means any data that serves to describe as fact a condition, circumstance, event, transaction, attribute, or process, whether or not determined to be factually accurate. A very large amount of factual data is recorded in logs, describing events or transactions that have occurred within information systems (including extensions of those systems as distributed systems operating across Internet-based networks).

Fictional Data means any data that is intended to describe fictional conditions, circumstances, events, transactions, attributes, or processes. Examples include creative works such as poetry, novels, films, audio recordings, etc., that are the primary focus of global copyright laws. Fictional data also includes data that is offered as factual but demonstrated to not be factual in truth by a defined calculation process using probability mathematics.

---

[6] What information may be defined as personally identifiable information varies across international, national, and state laws. For example, the General Data Protection Regulation (GDPR) adopted by the European Parliament, which becomes effective in May, 2018, defines "personal data" to mean ". . . any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. By contrast, the U.S. has no formal statutory definition; the Office of Management and Budget states in a memorandum directed to Federal agencies that

PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES: PREPARING FOR AND RESPONDING TO A BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (2017), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, at 8.

These terms serve several purposes. First, the list itself highlights that personal information is merely a subset of the data being created by humankind, our systems, and our machines. We contend that further regulation of personal information that fails to align to, and share a common foundation with, industrial data (which is factual data) and fictional data will exacerbate rather than improve the effectiveness of regulating how industry manages personal information and accommodates the rights and controls of data subjects.

Second, these terms do not embrace the existing structures of copyright laws which, responding to digital media and digital information, have been amended, construed by courts, and, ultimately, supplemented in some nations by explicit laws expressing the rights of those who create databases (and distinguishing those from copyright owners).[7]

Finally, the definitions present an explicit distinction between industrial data and personal information. Anonymization, pseudonymization, tokenization, filtering, masking, and similar techniques continue to evolve as "work-arounds" that limit the effectiveness of the rights of data subjects.[8] But once anonymization has served its purpose, the resulting data is truly functioning as industrial data. The distinctions in definitions will enable industrial data to be owned, transferred, and legally protected by distinct legal and commercial rules while also more fully achieving the goals of privacy and data protection laws to truly vest in data subjects meaningful control of their identifiable personal information.

II. CURRENT CALLS FOR DATA OWNERSHIP

This article was provoked by discussions in public media and conferences about the conflicts among legal systems regarding *ownership* of data and the impact of those conflicts in light of the GDPR.[9] One commentator noted, "Ownership of data, both personal and machine-

---

[7] As proposed *infra* Part V, the continued tension of trying to adapt copyright and trade secret laws to protect industrial data may be addressed by limiting copyright laws to fictional data (such as creative works—books, films, music, etc.) and revising trade secrets law and the new proposed structure to focus on factual data.

[8] *See, e.g.,* Clyde Williamson, *Pseudonymization vs. Anonymization and How They Help with GDPR,* PROTEGRITY BLOG (Jan. 5, 2017), http://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/ (explaining the differences between anonymized and pseudonymized data and their relevance to compliance with the GDPR); *see also* BALAJI RAGHUNATHAN, THE COMPLETE BOOK OF DATA ANONYMIZATION: FROM PLANNING TO IMPLEMENTATION (2013) (offering an integrated view of how anonymization processes work).

[9] *See, e.g.*, Zenobia Hedge, *Privacy and Data Ownership as a European Business Advantage*, IOTNOW (Dec. 21, 2016), https://www.iot-now.com/2016/12/21/56731-privacy-and-data-ownership-as-a-european-business-advantage/.

generated, is at the core of the data-driven economy."[10] That statement is deceptive in its simplicity; if ownership itself is not recognized and enforceable under the rule of law, then the vitality, integrity, and potential of the "data-driven economy" is at risk.

From legal, contractual, and economic perspectives, numerous questions arise. As a general proposition, no privacy or data protection laws expressly define which entity *owns* personal information.[11] So, the following questions appear to apply both for industrial data and personal information: How should ownership of data be defined, if at all? When does ownership attach to data? Are there pre-conditions or criteria (such as originality, level of effort, or imposition of security controls) to be satisfied before ownership will be deemed to be attached to specific data? What are the rights, privileges, controls, and constraints that data ownership vests in the owner? How may those rights, privileges, and controls be transferred or regulated by contracting tools (such as purchase agreements and licenses)? What tools, mechanisms, or processes exist (or can be imagined) that may automatically enforce the rights, privileges, and controls of data ownership across distributed, complex information systems? Do existing, conflicting legal treatments of industrial data under copyright and database laws continue to work if clear ownership itself is defined now as an explicit starting point? How do certainty of ownership and the legitimate exercise of controls on the rights of ownership affect how data is economically valued as an asset of any company, business, or operating entity?[12]

All of these are challenging questions. For this article, we surveyed how, if at all, these questions are being answered amidst the current calls for data ownership to be established. As one scholar described the situation, we are facing "a series of as yet 'unknown unknowns' . . . a framework of law (as distinct from regulation) based on the clear definition of property rights is the best way to lay foundations for future economic success."[13] While we attempted to review the full portfolio of discussions of data ownership and property rights, our focus was on three nations and one international organization: Germany, Japan, Estonia, and the Organization for Economic Co-Operation and Development (OECD).

---

[10] *See* Williamson, *supra* note 8.

[11] Whether property rights are a suitable construct for personal information has been vigorously discussed in academic literature in both the EU and the United States. *See infra* Part III.

[12] "Infonomics" is a term coined by Doug Laney, Vice President and Distinguished Analyst at Gartner. *See generally, e.g.* DOUGLAS B. LANEY, INFONOMICS: HOW TO MONETIZE, MANAGE, AND MEASURE INFORMATION AS AN ASSET FOR COMPETITIVE ADVANTAGE (2017). His work on monetizing data as an economically valued asset has been at the cutting edge of advancing the dialogue on how to value data. *Id.*

[13] EBEN WILSON, DIGITAL DIRIGISME A RESPONSE TO DIGITAL BRITAIN (2018).

A. German Strategies and Innovations

Germany's political leadership has discussed data ownership explicitly; there is also substantive research toward new innovations underway and legal reform proposals.

In March 2017, ahead of CeBit,[14] the world's biggest information technology trade fair, German Chancellor Angela Merkel used a podcast to call for rules for data ownership.[15] She recognized the importance of establishing „möglichst vergleichbare Rechtslagen in allen europäischen Ländern"[16] and besides the „Datenschutzgrundverordnung [, die] ganz wichtig für Europa [ist]," the current discussion needs to focus on „eigentumsrechtliche Fragen."[17] In her remarks, Chancellor Merkel made a strong connection between the need for rules over data ownership and the innovation potential and international competitive ability of the German and European economy. Viewing the automotive industry as a driving force in the German economy („Deutschlands Zugpferd der Wirtschaft"),[18] Angela Merkel observed the need of regulation over data ownership: „[E]s ist natürlich wichtig, ob dem Autohersteller die Dinge gehören, oder ob dem Softwarehersteller die Daten gehören. Denn mit den Daten über die Nutzer wird man natürlich wieder neue Produkte und Anwendungen herstellen können. Und da, glaube ich, alles was Urheberrecht, was Eigentum an Daten anbelangt, da müssen wir noch die Rechtssetzung in Europa sehr schnell und sehr einheitlich durchführen."[19]

---

[14] CeBIT, http://www.cebit.de/en/#new-cebit (last visited Aug. 24, 2017) (describing itself as "Europe's Business Festival for Innovation and Digitization").

[15] Byomakesh Biswal, *Ahead of CeBit Visit, Merkel Calls for Rules Over Data Ownership*, COMPUT. BUS. REV. (Mar. 20, 2017), http://www.cbronline.com/news/verticals/central-government/cebit-visit-merkel-calls-rules-data-ownership/.

[16] The quote translates to: "preferably comparable legal situations in all European countries." VIDEO-PODCAST DER BUNDESKANZLERIN #10/2017 (2017), *available at* https://www.bundeskanzlerin.de/Content/DE/Podcast/2017/2017-03-18-Video-Podcast/links/download-PDF.pdf?__blob=publicationFile&v=4.

[17] [Questions of ownership]. *Id.*

[18] For a more detailed but brief analysis (in German) of the importance of the automotive industry, see *Die Deutsche Automobilindustrie—Im Ausland Weiter Auf Der Überholspur [The German Car Industry-On the Fast Lane Abroad]*, PRICEWATERHOUSECOOPERS (Sept. 25, 2015), https://www.pwc.de/de/internationalisierung/die-deutsche-automobilindustrie-im-ausland-weiter-auf-der-ueberholspur.html (confirming Merkel's description of the automotive industry as the "driving force of the German economy").

[19] [But of course, it is important [the question of ownership], whether the things [data] belong to the car producers or to the software producer. Because by using the date of the user it is possible to produce new products and applications. And at that point, I believe, we need a lawmaking for copyright law, for ownership of data, in

1. Datenausweis for Digital Sovereignty

Alexander Dobrindt, Federal Minister of Transport and Digital Infrastructure, proposed a new law in March 2017 that aligns with Angela Merkel's podcast statement. He calls for a „Datensouveränität des Einzelnen."[20] The minister's proposed data law includes five distinctive principles.

First, data should have the same legal status as material commodities, to assure data can be allocated as property towards a natural person or a legal entity. Second, the data should belong to the person to which the data pertains. If the user does not accept the usage of his or her personalised data, the processing and networking of that data needs to be anonymous and pseudonymous. The power of revocation must be accorded.[21] Third, people should have the chance to make informed decisions on the usage of their data. For this, transparent information is needed which all services and products must guarantee and a data license should include all information about the frequency of collection as well as the usage and disclosure of data. Fourth, public data is to be considered as open data. All non-personalised data which is collected by the state should be an open source to ensure a digital value creation. Finally, as an

---

Europe very soon and in a very coherent manner (when it comes to comparable national legal situations).]

Merkel, Angela: Rede von Bundeskanzlerin Merkel zur Eröffnung der CeBIT 2017 am 19. März 2017, available at https://www.bundesregierung.de/Content/DE/Rede/2017/03/2017-03-19-rede-merkel-cebit.html. By contrast, in the opening speech for CeBit on March 19, 2017 Merkel did not explicitly speak about the regulation of data ownership. But by referring to the achievements of Japan, the guest country of this year's exhibition, she says „Gemeinsam müssen – hier nehme ich das Angebot von Shinzō Abe sehr gern auf – *Standards* für die Vernetzung der Dinge entwickelt werden." ("Together we need—and here I embrace Shinzō Abe's offer—to develop standards of the Internet of Things"). Both countries have, according to Merkel, the same expectations of a social economy with the „Mensch und seine Lebensbedingungen" ("individual and his/her living conditions") in the center. In her speech she also asked: „Bin ich ein Datenlieferant, mit dessen Daten alles Mögliche gemacht wird, oder welchen Schutz und welche eigene Beeinflussungsmöglichkeit habe ich?" ("Am I a supplier of data with whose data everything can be done or what protection or possibility of influence do I have?"). CeBIT, *supra* note 14. Though she does not explicitly call for regulation over data ownership the terminus "Beeinflussungsmöglichkeit" [possibility of influence] gives a hint towards standardizations or regulations.

[20] [Data sovereignty for the individual]. *Wir Brauchen Ein Datengesetz in Deutschland! [We Need a Data Law in Germany!]*, BUNDESMINISTERIUM FÜR VERKEHR UND DIGITALE INFRASTRUKTUR, https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html (last visited Aug. 24, 2017).

[21] There is no indication that Dobrindt was limiting this concept to human individuals, but the principle certainly is consistent with GDPR.

alternative to the open availability of data, users should get the alternative to choose other payment solutions.[22]

While German newspapers[23] mostly wrote about the *Datenausweis* as a tool for data ownership of car drivers, according to the Ministry of Transport and Digital Infrastructure, its cornerstones should be for all „Dienste und Produkte."[24]

As recently as August 2017, a new study was published by the Ministry of Transport and Digital Infrastructure that focused on the mobile phone and related data. That study also confirmed, at present, there is no "data ownership" by the person. „Die verschiedenen Anknüpfungspunkte von verschiedenen Personen stehen in einem bisher nicht auflösbaren Widerspruch."[25]

2. Industrial Data Space

The Industrial Data Space (IDS) is a research project funded by the German Federal Ministry of Education and Research, closely associated with a member organization of companies, Industrial Data Space e.V.[26] The

---

[22] *Wir Brauchen Ein Datengesetz in Deutschland!*, *supra* note 20. In addition to aligning to property rights concepts, the latter principles reflect concepts of transparency and availability consistent with privacy law principles.

[23] *See Dobrindt Schlägt Datenausweis für Vernetzte Fahrzeuge Vor [Dobrindt Suggests a Data License for Interconnected Vehicles]*, ZEIT ONLINE (Mar. 20, 2017, 4:18 PM) http://www.zeit.de/news/2017-03/20/deutschland-dobrindt-schlaegt-datenausweis-fuer-vernetzte-fahrzeuge-vor-20161803; *Verkehrsminister: Dobrindt will „Datenausweis" für Autos [Minister for Mobility wants a "Data License" for cars]*, AUTOMOBILWOCHE (Mar. 20, 2017, 5:00 PM) http://www.automobilwoche.de/article/20170320/AGENTURMELDUNGEN/303209932/verkehrsminister-dobrindt-will-datenausweis-fuer-autosee.

[24] *Wir Brauchen Ein Datengesetz in Deutschland!*, *supra* note 20. Those outside of Europe should also take note that Germany has given digital infrastructure a Cabinet-level priority, something distinctively absent in many other developed economies.

[25] "Different starting-points of different legal entities are in a not yet solved contradiction." BUNDESMINISTERIUM FÜR VERKEHR UND DIGITALE INFRASTRUKTUR, „EIGENTUMSORDNUNG" FÜR MOBILITÄTSDATEN? [SYSTEM OF OWNERSHIP FOR MOBILE DATA?], *available at* http://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile.

[26] BORIS OTTO, ET AL., INDUSTRIAL DATA SPACE: DIGITAL SOVEREIGNITY OVER DATA [sic] (2016), *available at* https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/whitepaper-industrial-data-space-eng.pdf; *see also, e.g.*, INDUSTRIAL DATA SPACE ASSOC., www.industrialdataspace.org (last visited Aug. 25, 2017); *Industrial Data Space*, DELOITTE, https://www2.deloitte.com/de/de/pages/innovation/contents/industrial-data-space.html (last visited Aug. 25, 2017).

IDS is developing integrated reference models using standards and common governance models.[27] These models are intended to enable data to be linked within and among business ecosystems and "*ensure[e] digital sovereignty of data owners*."[28] A 2016 white paper introduced several vital descriptions of the requirements of businesses against which the reference models are to be developed:

> *Data as a product*—As evidenced by the emergence of data marketplaces, data has become a product itself.[29]
>
> *Data sovereignty*—The data owner has "sovereignty," specifically the right to specify the terms and conditions of use for any data provided to others. The models contemplate the owner being able to 'attach' terms and conditions to the relevant data.[30]
>
> *Data economy*—Data is viewed as an economic asset and includes both "private data" (industrial data owned by a specific company) and "club data" (industrial data within a specific value creation chain available to selected companies).[31]
>
> *Data governance*—Companies jointly decide on data management processes as well as applicable rights and duties. IDS emphasizes that the distributed architecture they contemplate specifically needs "rules of the game" to be authored when there is no central supervisory authority.[32]

These concepts, of course, appear to align closely with the policy remarks made by German political leadership.[33] While the IDS white paper and later research do not specify how ownership and property rights originally vest with regard to specific data, their models contemplate that the derivative rights (access, use, levels of aggregation, downstream distribution, etc.) can be implemented as modules into the automated connections among users and other stakeholders such as data providers.[34]

---

[27] OTTO, *supra* note 26, at 4. Four architectures are contemplated, addressing business (including data governance, rights, and duties), security, data and services, and software.

[28] *Id.* (emphasis added).

[29] *Id.* at 10. Big data analytical services have also been creating financial exchanges for data. *See generally*, LANEY, *supra* note 12.

[30] *Id.* at 5.

[31] The connection between this vision of a value chain and the use of blockchain distributed ledger technologies must be emphasized. *See supra* Part V of this article. Data moves within business ecosystems that functionally chain together different data assets, services, and outputs derived from the data.

[32] OTTO, *supra* note 26, at 13.

[33] *See supra* text accompanying notes 15–26.

[34] *Id.* at 24; *see also* BORIS OTTO ET AL., REFERENCE ARCHITECTURE MODEL FOR THE INDUSTRIAL DATA SPACE (2017), *available at* https://www.fraun

The 2017 Reference Architecture Model illustrates that data ownership impacts every layer of the proposed architecture; however, while recognizing that possession and ownership are different concepts, particularly for digital ecosystems, there is not yet further guidance on how ownership attaches to data itself.[35]

B. Japanese Strategies and Innovations for Data Markets

Japan's government also has been conspicuous and productive in its focus on digital strategies. Recent work emphasizes the role of contracts in expressing and governing the rights of commercial parties in industrial data.

1. Contracting for Data Utilization

Japan's Ministry of Economy, Trade and Industry (METI) has produced a number of important policy documents on digitalization strategy and innovations that emphasize its appetite for clear rules on the ownership of data. Its focus is substantive and significant, including expressing the leadership by a Director General for International Cyber Economic Policy.[36]

METI, in May 2017, published Contract Guidelines on Data Utilization Rights ver. 1.0.[37] These Guidelines aim to encourage businesses to clarify data utilization rights by drafting "proper contracts." Use cases for the Guidelines focus on manufacturing company interactions with industrial data, specifically operating data generated from machine tools used in manufacturing and analytical business data from service providers.

Under Japanese law,

> "[D]ata is intangible and not subject to ownership under the Civil Code. Non-personal data may in principle be freely used . . . except for legally protected intellectual property falling under copyright, trade secret or other legal statutes."[38]

---

hofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/Industrial-Data-Space_Reference-Architecture-Model-2017.pdf.

[35] OTTO ET AL., *supra* note 34, at 70.

[36] *See* CEBIT ET AL., HOW DIGITAL TRADE CAN SUPPORT BUSINESS TOWARDS AND OPEN AND FAIR BUSINESS ENVIRONMENT 2 (2017), *available at* http://cdnsite.eu-japan.eu/sites/default/files/imce/seminars/2017-03-20-CeBIT/20170320-cebitreport.pdf (stating that Director General for International Cyber Economy Policy at the Japanese Ministry for Economy, Trade and Industry, Kiyoshi Mori, gave the keynote speech) [hereinafter DIGITAL TRADE REPORT].

[37] *See generally Contract Guidelines on Data Utilization Rights ver. 1.0 Formulated*, METI (May 30, 2017), http://www.meti.go.jp/english/press/2017/0530_002.html [hereinafter METI GUIDELINES].

[38] METI, BACKGROUND TO THE FORMULATION OF CONTRACT GUIDELINES ON DATA UTILIZATION RIGHTS VER. 1.0 (2017), *available at* http://www.meti.go.jp/english/

As a result, contracts are recognized as a controlling source of the rules for how data may be utilized within commercial relationships. Yet recently, METI concluded that existing contracts were insufficient.

The Guidelines offered two observations: "Data ownership is often not clarified among businesses" and "Data utilization rights (data ownership) are not necessarily properly or fairly specified in contracts depending on the nature of the data.[39] In practice, data is being utilized without clarifying the particular associated rights." Overall, "a lack of clear definitions and terms for data use in contracts between business partners hinders businesses from making progress in concluding contracts."[40] The Contract Guidelines are awaiting translation into English but are now available in Japanese.[41]

An English-language summary states that model contract clauses are included in the Guidelines, emphasizing that data utilization rights should be "examined fairly and objectively" and take account of the levels of contribution toward creation, preservation, management, and how the data will be utilized.[42] The summary emphasized that "Data utilization right [sic] is not always vested in one party."[43]

In related press coverage, *Nikkei* reported that the guidelines urge companies to clarify, when buying business equipment or entering into business partnerships, who has the rights to the data and how the proceeds from big data will be shared. Automotive (including tires, in-car electronics, and self-driving vehicles), machine tools, and building maintenance are highlighted as big data intensive industries.[44] Central to the collective efforts sponsored by METI is the potential for non-monopolistic data

---

press/2017/pdf/0530_002b.pdf. For our purposes, we accepted this summary of Japanese law without independent verification.

[39] *Id.*

[40] *See* METI GUIDELINES, *supra* note 37.

[41] METI, DĒTA NO RIYŌ KENGEN NI KANSURU KEIYAKU GAIDORAIN [CONTRACT GUIDELINES ON DATA UTILIZATION RIGHTS], http://www.meti.go.jp/press/2017/05/20170530003/20170530003-1.pdf (last visited Dec. 27, 2017).

[42] METI, OUTLINE OF CONTRACT GUIDELINES ON DATA UTILIZATION RIGHTS VER. 1.0 (2017), *available at* http://www.meti.go.jp/english/press/2017/pdf/0530_002a.pdf. Full versions of the model language in English are not yet available.

[43] *Id.*

[44] *Japan to Urge Businesses to Share Big Data*, NIKKEI ASIAN REV. (Apr. 3, 2017, 3:00 AM), https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-to-urge-businesses-to-share-big-data.

sharing among industrial collaborators to enhance innovation and overall industrial efficiency.[45]

2. Study of the Fourth Industrial Revolution

Under the auspices of METI, Japan developed its *Japan Revitalization Strategy 2016*.[46] In furtherance of that strategy, the Cross-Sectional System Study Group for the Fourth Industrial Revolution produced a report.[47] This Report emphasized the economic, functional, and strategic importance of data, specifically industrial data, to the rapid evolution of the "Fourth Industrial Revolution."[48] Two classes of data are highlighted by the Study Group: virtual data, which emphasizes data that is inferred from online behavior, and real data, such as that which sensors from industrial operations generate.[49]

The Report describes how online transaction platforms and business operators are not only collecting and using information from their own platforms but seeking out data from other platform and business operators that may enrich and enhance their own data. The Report endorses developing a data distribution market that enables data collected by one platform or business to be more easily exchanged and exploited in order to promote innovation and economic growth. Standards, improved verification, and technology developments; developing rules for "whitelisting" selected data sets (and, logically, sources) to accelerate transaction efficiency; and guidelines and sample clauses for transactional agreements—all are identified as useful building blocks.

As for industrial data, the Report considers "[c]lassification of rights between the parties involved (including possession of the deliverables of data analysis) as a precondition to [smoother data distribution]." Indeed, the Report is quite explicit on the additional building blocks for industrial data, including: "[a]ccurately understanding the current state including what data are stored and where, and which agreement applies to the provision of data is required"; "[d]evelopment of a system of intellectual property rights

---

[45] *Id.*; *see also* George Hill, *Could Japan's Approach to Data Sharing Change the World?*, INNOVATION ENTER. (Apr. 3, 2017), https://channels.theinnovationenterprise.com/articles/could-japan-s-approach-to-data-sharing-change-the-world.

[46] METI, JAPAN REVITALIZATION STRATEGY 2016 (2016), *available at* https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/hombun1_160602_en.pdf.

[47] *See generally* METI, REPORT OF THE CROSS-SECTIONAL SYSTEM STUDY GROUP FOR THE FOURTH INDUSTRIAL REVOLUTION (PROVISIONAL TRANSLATION) (2016), *available at* http://www.meti.go.jp/english/press/2016/pdf/0915_02c.pdf [hereinafter REPORT].

[48] *Id.*

[49] *Id.*

related to data and databases;" and "[u]nderstanding of the current state of contracts regarding intercorporate data transfers."

While expressed in terms of intellectual property and copyright, more detailed discussion in the Report emphasizes that the envisioned data distribution market requires clearly defined rules regarding the rights and privileges of data under the control of platform and business operators. The promotion and sharing of data is encouraged, in large part, to strengthen competitive advantage for existing and new businesses. International standards are encouraged for development, including how companies may identify and express the rights relating to certain data and conditions which may influence the exercise of those rights.[50]

In addition, while acknowledging that databases are protected in Japan by the Copyright Act and that the Unfair Competition Prevention Act also provides trade secret protection of the related creativity and confidentiality, the Report shares contributed comments that "protection outside the existing system is necessary; and not intellectual property rights *but access rights or rights of utilization may be practical for data)*."[51]

In summary, several elements of the Study Group Report are worth emphasizing. The Report recognizes the emergence of industrial data as a resource of economic, functional, and strategic value. But the Report concludes that existing legal systems are insufficient to support the emergence of a data distribution market and that new rules are required. Those rules need to focus on rights, conditions, and commercial agreements (in the words of the Report: "Appropriate rights protection is required for these [new data sharing] technologies and database[sic]."). That seems to confirm the importance of defining rights of use and access without regard to whether the data is personal data or industrial data.[52]

3. Japan Business Council in Europe and EU-Japan Centre for Industrial Cooperation

The Japan Business Council in Europe and the EU-Japan Centre for Industrial Cooperation issued a report in March 2017 emphasizing their mutual, shared progress toward "digital trade" and the development of a "predictable and seamless framework for the digital economy."[53] The report, and the substantive work described in its pages, emphasizes the

---

[50] *See infra* Part V. The proposal offered in Part V is intended to support these building blocks being achieved.

[51] REPORT, *supra* note 47, at 28 (emphasis added).

[52] *Id.* at 27. METI has continued to make progress supporting research toward data utilization and improving distribution environments; *see also Guidelines for Concluding Contracts with Credit Card Affiliated Stores Formulated*, METI (July 3, 2017), http://www.meti.go.jp/english/press/2017/0703_003.html.

[53] DIGITAL TRADE REPORT, *supra* note 36, at 1.

cross-continental work being done to move beyond current digitally-intensive business models toward further innovation.[54] Among other topics, the report described the joint EU and Japanese government commitments to include data flow issues and cooperation on the data economy in the negotiations of a comprehensive Economic Partnership Agreement/Free Trade Agreement (EPA/FTA).[55]

C. Estonian Strategies and Innovation

Estonia is Europe's most entrepreneurial hotspot,[56] with start-ups such as Skype[57] and Transferwise.[58] The most Northern Baltic state is a digital forerunner not only in Europe but worldwide when it comes to digitalization. As a "Baltic Tiger"[59] that was able to radically change its administration towards an e-governance of the 21st century, Estonia is a "digital zoo"[60] visited by national delegations from all over the world, with innovative approaches such as the establishment of data embassies[61] abroad

---

[54] This event report, emphasizing German-Japanese collaboration, should be considered alongside the analysis in the final section of this Part II on the data sharing innovations and developments among the automotive manufacturers from those two nations.

[55] *Id.*

[56] Alex Gray, *Europe's Most Entrepreneurial Country? It's Not the One You Might Expect*, WORLD ECON. FORUM (Mar. 16, 2017), https://www.weforum.org/agenda/2017/03/europes-most-entrepreneurial-country/.

[57] Isabelle de Pommereau, *Skype's Journey from Tiny Estonian Start-up to $8.5 Billion Microsoft Buy*, CHRISTIAN SCI. MONITOR (May 11, 2011), https://www.csmonitor.com/World/Europe/2011/0511/Skype-s-journey-from-tiny-Estonian-start-up-to-8.5-billion-Microsoft-buy.

[58] *See Welcome to Money Without Borders*, TRANSFERWISE, https://transferwise.com/us/about (last visited Dec. 27, 2017) (noting that the company's founder worked for Skype Estonia).

[59] *See generally* FREDERIK ERIXON, EUROPEAN CTR. FOR INT'L POLITICAL ECON, THE BALTIC TIGER: THE POLITICAL ECONOMY OF ESTONIA'S TRANSITION FROM PLAN TO MARKET (2008), *available at* http://www.ecipe.org/app/uploads/2014/12/the-baltic-tiger.pdf (describing Estonia as the "Baltic Tiger").

[60] *See* Ingmar Volkmann, *Wunderdinge aus dem Silicon Valley Europas*[Miracles from the European Silicon Valley], STUTTGARTER-ZEITUNG (Oct. 27, 2017, 5:57 PM), http://www.stuttgarter-zeitung.de/inhalt.estland-als-digitaler-vorreiter-wunderdinge-aus-dem-silicon-valley-europas.f325b055-c099-4211-af53-d725b90f1f0f.html.

[61] *See Estland: Regierungschef Ratas verlagert seine digitale Verwaltung ins Ausland [Estonia: Head of Government Ratas Relocates His Digital Administation Abroad]*, FUTUREZONE.DE TECH. NEWS (June 21, 2017, 7:50 AM), https://www.futurezone.de/netzpolitik/article210981221/Estland-Regierungschef-Ratas-verlagert-seine-digitale-Verwaltung-ins-Ausland.html; *E-Residency*, REPUBLIC OF ESTONIA, https://e-resident.gov.ee (last visited Dec. 27, 2017).

or e-residency receiving attention.[62] Estonia is illustrative of what governments of other nations might implement in the closer digital future.[63]

Yet research was not able to locate any published formal discussion of the concept of data ownership in Estonia's Civil Code or related legal materials. However, the Civil Code introduces an interesting categorization of how legal rights and transactions are to be structured based on the objects of the transaction.[64] Estonian law recognizes three different objects: goods, rights, and other benefits which can be the object of a right.[65] "Property" may also include a set of monetarily appraisable rights and obligations belonging to a person.[66]

However, a right of ownership is a real right, as expressed in the Law of Property, and can be established only in the cases provided by law.[67] While there is no guidance available on the applicability of these concepts to digital information, the possibility exists to argue the rights of control for data might be an "object" that can be the basis for a commercial transaction. Of course, that approach is, at this point, merely speculative. But the Code-

---

[62] *See, e.g., Estonia is Trying to Convert the EU to its Digital Creed*, https://www.economist.com/news/europe/21724831-country-e-residency-wonders-why-others-are-more-sceptical-estonia-trying-convert (last visited Jan. 25, 2018); *Estonia Sets the Standard for a Digital Democracy*, http://www.smartmatic.com/news/article/estonia-sets-the-standard-for-a-digital-democracy/ (last visited Jan. 25, 2018).

[63] *See, e.g.*, *Building Blocks of Estonia*, REPUBLIC OF ESTONIA, https://e-estonia.com/solutions/ (last visited Dec. 27, 2017) (stating additional details on e-Estonia); *see also* Samburaj Das, *100%: Dubai Will Put Entire Land Registry on a Blockchain*, CRYPTOCOINSNEWS (Oct. 9, 2017, 1:01 PM), https://www.cryptocoinsnews.com/100-dubai-put-entire-land-registry-blockchain/. Dubai is another jurisdiction pursuing digital transformation of government services. *Id.*

[64] The authors note, with appreciation, the assistance of Triin Siil in providing guidance on the specific provisions of Estonian law summarized here.

[65] *See* General Part of the Civil Code Act (GPCCA) §§ 48–50 (2017) (Estonia); *see also* RIIGI TEATAJA, https://www.riigiteataja.ee/en/?leht=7&kuvaKoik=false&sorteeri=avaldamiseKp+id&kasvav=false (last visited Dec. 27, 2017) (providing English translations of the GPCCA).

[66] *See* General Part of the Civil Code Act (GPCCA), § 66 (2017) (Estonia); *see also* RIIGI TEATAJA, https://www.riigiteataja.ee/en/?leht=7&kuvaKoik=false&sorteeri=avaldamiseKp+id&kasvav=false (last visited Dec. 27, 2017) (providing English translations of the GPCCA). The concept of appraising value in monetary terms is fascinating to contemplate: How much is data worth? How is that value calculated? What measures are invoked? What qualities can influence the value calculations? These questions are beyond the scope of this article but vital to how digital markets will evolve.

[67] Law of Property Act § 68(1), § 68(3) (2017) (Estonia); *see also* RIIGI TEATAJA, https://www.riigiteataja.ee/en/eli/ee/526012017002/consolide/current (last visited Dec. 27, 2017) (providing English translations of the Law of Property Act).

based recognition of rights highlights how critical it is that there be greater certainty in what those rights are for any specific data asset. At the same time, the fact that ownership rights must be explicit also underscores the potential value with which those ownership rights are viewed explicit.

D. Organization for Economic Cooperation and Development

The OECD has been actively contributing to the strategic analysis required to advance digital markets and economies. It has consistently expressed awareness of the need for reform in the legal infrastructure for data, including in these key reports summarized below.[68]

1. Key Issues for Digital Transformation in the G20

In January 2017, the OECD issued a 150+ page report, *Key Issues for Digital Transformation in the G20*.[69] The Report was prepared by the OECD Secretariat at the request of the G20 German Presidency. It is the most detailed, thorough presentation on the reforms in regulation and legal frameworks required to enable the digital economy reviewed by the authors. Building "advanced governance frameworks" is described as "necessary to effectively address the complexity of today's interlinked issues in successful Industrie 4.0 development and deployment."[70]

One key barrier identified is the awareness that the exclusive rights and control held by an owner of physical goods have *not* been extended to data. While intellectual property rights (such as copyright, database protection laws, and trade secrets) "can be used to a limited extent," more is required to enable "different stakeholders having different rights" to be properly exercised. The scope of those rights is described to include "the ability to access, create, modify, package, derive benefit from, sell or remove data, [and] the right to assign these access privileges to others."[71] Indeed, data ownership and IPRs are identified as a barrier to investments in new data assets and the capabilities of those assets in commerce and industry.[72]

---

[68] *See* OECD, KEY ISSUES FOR DIGITAL TRANSFORMATION IN THE G20, 150–62 (2017), *available at* https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf (including a detailed bibliography of OECD work product on digitalization and Industrie 4.0).

[69] *See generally id.*

[70] *Id.* at 8; *see also id.* at 73–81.

[71] *Id.* at 65–66; *see also* DAVID LOSHIN, PROCEEDINGS OF THE 2002 ACM CIKM INTERNATIONAL CONFERENCE ON INFORMATION AND KNOWLEDGE MANAGEMENT, RULE-BASED DATA QUALITY 614–16 (2002), *available at* http://doi.acm.org/10.1145/584792.584894.

[72] OECD, *supra* note 68, at 66.

Nearly unique among the reports that were studied was an awareness to the potential for the data generated by autonomous machine-to-machine communications, balanced against the barriers that exist to making the necessary investments.[73]

The Report also concludes that "sound regulatory frameworks . . . that enable digitalisation are essential" to foster innovation by small to medium sized enterprises (SMEs).[74] While emphasizing the importance of developing open standards for technical aspects of Industrie 4.0, the Report recommends that countries develop mechanisms to periodically review their legal frameworks and update them to be responsive to the increasingly digitalised world.[75]

2. Trade Union Advisory Committee

In February 2017, the OECD Trade Union Advisory Committee published an analysis of key issues and recommendations regarding the continuing growth of the digital economy. Emphasizing the goal of fostering progress, the Committee recommended that digital innovation will succeed when based on rules on intellectual property rights that address, among traditional patent and copyright topics, the rights to access, process and delete data, as well as "the right to access digital platforms."[76]

The Committee also addressed data governance, noting that it is important to create better data governance regimes and legal rules. To achieve that objective, "standards on data ownership including the right to access, process, and deletion, and on the pricing of data" are recommended.[77]

E. Summary

This review of German, Japanese, and Estonian developments, as well as the OECD reports, confirms several observations.

First, there is substantial recognition that industrial data has economic and functional importance to the future of digital economies and markets. Data sharing, in order to enable efficiency and innovation, is clearly valued as an outcome to be achieved by improved concepts of data ownership and data governance.

---

[73] *Id.* at 65.
[74] *Id.* at 124.
[75] *Id.*
[76] TRADE UNION ADVISORY COMMITTEE, DIGITALISATION AND THE DIGITAL ECONOMY: TRADE UNION KEY MESSAGES 2 (2017), *available at* https://www.ituc-csi.org/IMG/pdf/1703t_tu_key_recommendations_digitalisation.pdf.
[77] *Id.*

Second, both Germany and Japan recognize the monetary value their economies can create through new innovations and data markets based on a regulation of data ownership.

Finally, while ownership is viewed as an important foundational concept on which transactions in digital information can proceed, none of the materials surveyed propose an answer to the questions presented at the outset of this Part II. However, Japan and the EU-Japan cooperative efforts seem to have progressed furthest toward formulating those answers. In addition, there is formal awareness that the existing structures of copyright and database laws are insufficient to sustain the full potential envisioned for Industrie 4.0.

While other jurisdictions and organizations were examined,[78] none of the materials offered any contradictions of the preceding observations.

F. Data Ownership in the Automotive Industry

Encouraged by the ministerial and policy analyses summarized above, our research narrowed onto the automotive industry to evaluate the degree to which the issues of data ownership and propertization have evolved. Globally, the industry, including both major Japanese and German manufacturers, is accelerating the digitalization of the automobile to support both driverless vehicles and increased tracking of travel and performance.

In 2015, the World Economic Forum published an analysis, *Who Owns Connected Car Data?*[79] Summarizing industry-focused innovations, the Report noted that the technologically self-aware vehicle creates an operating environment in which all vehicles sense each other and, in turn, generate, store, and share immense amounts of data to enable their efficient and safe operation. In asking the title question, the report observed, "The issues are deceptively thorny."[80] Yet, as summarized in a 2016 KPMG

---

[78] Additional materials that were examined include those from the European Union (including the Directorate-General for Communications Networks, Content and Technology, and the European Interoperability Framework), India, Italy, Serbia, Malta, France, Great Britain, the Netherlands, United States, and the Bank for International Settlements. Detailed references are available on request.

[79] Matthew DeBord, *Who Owns Connected Car Data?*, WORLD ECON. FORUM (Sept. 28, 2015), https://www.weforum.org/agenda/2015/09/who-owns-connected-car-data/. Similar media coverage has highlighted the competitive battles among the different stakeholders. *See, e.g.*, Keith Crain, *Who Owns Vehicle-Generated Data?*, AUTO. NEWS (May 11, 2015, 12:01 AM), http://www.autonews.com/article/20150511/OEM11/305119969/who-owns-vehicle-generated-data?; Matt Asay, *Tech Giants vs. Automotive Titans: The Battle for Your Car's Data*, TECHREPUBLIC (Dec. 7, 2015, 11:47 AM), http://www.techrepublic.com/article/tech-giants-vs-automotive-titans-the-battle-for-your-cars-data/.

[80] DeBord, *supra* note 79.

report on the connected car, "What's clear is this: Those who own the data win."[81]

The data produced, and capable of being produced, from the operation of automobiles and trucks and lorries is immense.[82] Sensors monitoring mechanical and electronic components to populate dashboard displays; event data recorders;[83] and linkages between mobile phones and automobiles to enable messaging, audio reminders, and oral conversations pale in significance to the operational industrial data that is generated by a self-driving vehicle.[84] Much of the data is industrial data, irrelevant to the operator or owner's identity, but invaluable to analytics, maintenance, performance evaluation, safety, innovations, and much more. To the extent the data can be identifiable to the operator or owner, a PII classification is appropriate.

The automobile becomes an archetypical example of the fact that nearly any device will consist of two assets: the physical equipment itself and the data generated from its operation. This is true for cars, trucks, locomotives, airplanes, drones, Internet of Things (IoT) devices, industrial

---

[81] KPMG, YOUR CONNECTED CAR IS TALKING. WHO'S LISTENING? (2016), *available at* https://assets.kpmg.com/content/dam/kpmg/br/pdf/2016/11/your-connected-car-is-talking.pdf.

[82] It is estimated that a manufacturer may need to manage 1030 theoretical product variants (headlights and outside mirrors may touch 40 or more alone). Otto, *supra* note 26, at 9.

[83] *See infra* Part II, *Data Rights Ownership in Automotive Event Data Recorders*.

[84] Studies are reporting self-driving, autonomous vehicles will generate up to four terabytes per day; others report a rate of 25 gigabytes per hour. *See, e.g.*, *Connected Cars Will Send 25 Gigabytes of Data to the Cloud Every Hour*, QUARTZ, https://qz.com/344466/connected-cars-will-send-25-gigabytes-of-data-to-the-cloud-every-hour/ (last visited January 25, 2018); Patrick Nelson, *Just One Autonomous Car Will Use 4000 GB of Data/Day*, NETWORK WORLD (Dec. 7, 2016, 7:39 AM), http://www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html; Peter Campbell, *UK Urged to Clarify Data Rules from Connected Cars*, FIN. TIMES (July 3, 2017), https://www.ft.com/content/0ebdd2aa-5dc5-11e7-9bc8-8055f264aa8b?mhq5j=e1; Florian Leibert, *The Most Revolutionary Thing About Self-Driving Cars Isn't What You Think*, WORLD ECON. FORUM (June 14, 2017), https://www.weforum.org/agenda/2017/06/the-most-revolutionary-thing-about-self-driving-cars-isn-t-what-you-think/ (stating that "[e]ach self-driving car is becoming its own powerful data centre" and highlighting that one of the key challenges is the speed at which computing must occur within the vehicle—a one second delay, at 65 mph moving speed, could be a life-or-death consequence).

manufacturing units, and so much more.[85] Overall, any associated PII is only a small slice of the overall data any of these devices will be producing.

It may be useful to delve into a fairly standard transaction set involving the assembly and sale of an automobile to illustrate the thorniness. The automotive manufacturer assembles each vehicle from a variety of components acquired by contract from subcontractors, including devices that act as data sensors, recorders, and communication units. Subcontractors may include both device suppliers as well as software developers that license software for installation in the vehicle (as well as paired applications enabling the data to be received and used by the manufacturer). Among the manufacturer and the subcontractors, who claims ownership to the data produced during the vehicle's operation? All would have good reasons to negotiate for the rights of ownership, including controlling the use of that data for analytics, product design and other uses unrelated to specific PII.

The vehicle is then sold to a commercial dealer. Does the dealer acquire any ownership interest in the data produced during operation? Until the vehicle is sold to a consumer, the dealer is the true owner; would that status not vest the dealer with rights to access and control the related operational data no different than the end consumer might claim to possess?

In wholesale and retail consumer transactions, the purchase price may be financed, either through a consumer loan or a lease (in which a leasing company purchases the car as the true owner, and then leases the vehicle to a consumer). Does the leasing company acquire the ownership rights to the data stream during the term of the lease? At this point, the consumer identity also can become tricky—even a true owner of the vehicle may not always be the operator. How will data associated with each operator be distinguished, and what will be their respective claims to their PII, as well as the other industrial data?

Insurance companies and governmental authorities have ongoing interests in being able to access the operational data generated by the automobile. For insurance companies (as well as financing lenders and leasing companies), the data has immediate use for assuring compliance with any conditions that may be a part of the related agreements (for example, conditioning insurance coverage on operation of the vehicle within defined geographic boundaries or at speeds not exceeding 105% of the posted speed limits). In these circumstances, the identity of the operator

[85] The National Football League is even placing data sensor chips in footballs used in professional games. Ken Belson, *NFL Expands Use of Chips in Footballs, Promising Data Trove*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/sports/nfl-expands-use-of-chips-in-footballs-promising-data-trove.html.

of the vehicle at any time, their respective rights in the operating data and their rights with respect to the related PII add additional complexity.

Other media coverage we surveyed highlights the type of questions for which the data can be useful in the event of a collision. Will parts suppliers be liable if the data indicates a related component failure? Was the use of autopilot suitable in the surrounding circumstances (such as extreme weather conditions)? Were brakes properly applied? Was the steering wheel at a suitable angle? Did the airbags properly deploy?[86]

There are also information security issues. Who is responsible for securing the systems and operational data from intrusion, exfiltration, or compromise? As well, there are further complexities of ownership when automotive systems connect to telecom systems or on-board entertainment devices such as OnStar or Sirius.[87] In our view, many of these questions can be resolved by clear, legally enforceable allocations of ownership and control among the various stakeholders.[88]

1. Data Rights in Automotive Event Data Recorders

Event data recorders installed in automobiles (EDRs) are similar to the black boxes installed in aircraft. They record data from sensors and systems within the vehicle and, when the EDRs detect an accident or collision, the related data is then stored and preserved for extraction and analysis. In 2010, significant public attention was drawn to the use of these devices and, in turn, media coverage reported on how Toyota used and disclosed the information.[89] Historically, while EDRs had been installed for

---

[86] *See* Crain, *supra* note 79. For recent liability issues relating to airbag deployment, *see, e.g.*, *Takata Airbag Recall – Everything You Need to Know*, CONSUMER REPORTS (July 14, 2017, 10:30 AM), https://www.consumerreports.org/cro/news/2016/05/everything-you-need-to-know-about-the-takata-air-bag-recall/index.htm. For information regarding unintentional accelerations, *see, e.g.*, Junko Yoshida, *Acceleration Case: Jury Finds Toyota Liable*, EE TIMES (Oct. 24, 2013, 9:00 PM), http://www.eetimes.com/document.asp?doc_id=1319897. For information regarding emission controls, *see, e.g.*, Guilvert Gates et al., *How Volkswagen's 'Defeat Devices' Worked*, N.Y. TIMES (Mar. 16, 2017), https://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html. All the related accidents involved in-car control systems and operational data was vital to the investigation and discovery of the related product defects.

[87] *See* KPMG, *supra* note 81.

[88] The KPMG report also describes an April 2016 negotiation breakdown among Apple, BMW and Daimler regarding questions of data ownership, cloud-based software, and data protection. *Id.*

[89] *See, e.g.*, Peter Whoriskey, *Event Data Recorders Used in NHTSA Study of Toyotas Have History of Problems*, WASH. POST (Aug. 20, 2010),

several years, Toyota was reported to refuse to disclose the data or would make only partial disclosures, including in litigation involving automotive safety claims.[90] State governments, including California, have enacted responsive regulations requiring notice and disclosures to consumers of the circumstances in which data may be downloaded from a vehicle's EDR, generally inside the user's manual that is delivered with the vehicle.[91]

Admittedly, there is a privacy element to the data collected by an EDR, but when EDR data is limited to accident-based collection (such as storing the data for the 30 second period prior to an event detected by the EDR), much of that concern is diminished. Indeed, when a collision has occurred, the public laws specifically confirm how regulators, investigators, and insurance companies may require access to, and obtain, the stored data. What the regulations seem to infer is that the automotive owner or operator controls the access and use to the collected data, but we explored how different manufacturers complied with the notice and disclosure rules regarding the data access and use rights to automotive owners, consistent with the regulatory requirement that they do so. The user manuals for the following automotive manufacturers were considered: Ford,[92] Toyota, Honda,[93] Porsche,[94] and BMW.[95]

Each manufacturer, with one exception, seems to faithfully reproduce the notices and disclosures that were mandated by public laws. Some variations occurred in how the language was presented, perhaps as a

---

http://www.washingtonpost.com/wp-dyn/content/article/2010/08/19/AR2010081906562.html.

[90] *See, e.g.*, Zachary L. Wool, *Toyota Hides Important Black Box Crash Data*, BARRIOS KINGSDORF & CASTEIX, L.L.P., http://www.bkc-law.com/blog/toyota-hides-important-black-box-crash-data/ (last visited July 24, 2017).

[91] The National Conference of State Legislatures has published a summary of this legislation. *See Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONF. OF STATE LEGS., http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx (last visited Aug. 10, 2017).

[92] FORD, FORD FOCUS 2017 OWNER'S MANUAL (2017), *available at* http://www.fordservicecontent.com/Ford_Content/Catalog/owner_information/2017-Ford-Focus-Owners-Manual-version-1_om_EN-US_EN-CA_10_2016.pdf.

[93] HONDA, 2008 PILOT ONLINE REFERENCE OWNER'S MANUAL (2008), *available at* http://techinfo.honda.com/rjanisis/pubs/OM/9V0808/9V0808OM.pdf.

[94] PORSCHE, PANAMERA OWNER'S MANUAL (2009), *available at* http://www.porsche.com/all/media/pdf/Owners_Manual_Panamera_PCNA.pdf.

[95] BMW, OWNER'S MANUAL FOR VEHICLE (2007), *available at* www.bmwusa.com/pdf_6ea435bc-898e-4455-90ac-0175dc04d47c.arox.

result of differences in the locations in which the vehicles are sold.[96] But the notices were complex, difficult to understand, and likely ineffective.[97]

The exception is noteworthy. In its notice, Honda, a Japanese-based manufacturer, stated specifically:

> This vehicle is equipped with one or more devices commonly referred to as event data recorders. These devices record front seat belt use, front passenger seat occupancy, airbag deployment data, and the failure of any airbag system component. ***This data belongs to the vehicle owner*** and may not be accessed by anyone else except as legally required or with the permission of the vehicle owner.[98]

This clear declaration of the automobile owner's ownership of the data is not required, but is both conspicuous and effective. Indeed, often, by its own terms, the manual is part of the contract between the manufacturer and the purchaser of the vehicle.[99] We find this example encouraging; it illustrates that data ownership can be affirmatively vested in an end consumer, while also clearly reserving the rights of designated third parties to access and use the stored data for defined purposes.[100]

G. The State of Law Regarding Data

The existing states of formal law regarding data ownership are both diverse, and often in conflict; many works of scholarship summarize these conflicts and report on the manner in which existing laws have evolved.[101]

---

[96] As with many consumer disclosures, manufacturers appear to work to consolidate into one notice and disclosure everything required by all of the jurisdictions.

[97] While the effectiveness of these specific notices has not been researched, their semantic structure and presentation are comparable at first glance to other notices regarding Internet websites and personal health information, the effectiveness of which has been researched and reported upon. *See, e.g.*, Matthew W. Vail et al., *An Empirical Study of Consumer Perception and Comprehension of Web Site Privacy Policy*, 55 IEEE TRANSACTIONS ON ENG'G MGMT. 442, 442–54 (2008); Ninghui Li et al., *A Semantics-based Approach to Privacy Languages*, 21 INT'L J. COMP. SYS. SCI. & ENG. 339, 339–52 (2006); Annie I. Antón et al., *The Lack of Clarity in Financial Privacy Policies and the Need for Standardization*, 2 IEEE SEC. & PRIVACY, 36–45 (2004).

[98] HONDA, *supra* note 93 (emphasis added).

[99] The Ford manual says "[this manual] is an integral part of your vehicle." FORD, *supra* note 92. Of course, this language does not resolve other questions raised in the preceding text regarding the ownership rights of non-owner operators, leasing companies, etc.

[100] This approach is exactly what is proposed *infra* Part V. Asserting and confirming the property rights in data need not conflict with the controls and constraints that a data subject (or similarly positioned corporate entity) may be entitled to assert with regard to the use of the data.

[101] Several of the most significant works are presented *infra* Part III.

For our purposes, it is sufficient to conclude here that there is no clear expression of ownership rights for digital data in the legal systems we reviewed in Europe, the United States, or other countries for which we surveyed summaries (available in English or German languages). Four essentials, however, are worth summarizing.

First, U.S. law, through an important decision of the Supreme Court, limits reliance on copyright law to protect databases of factual information, unless there is sufficient creativity in the development of the databases to justify copyright protection.[102] Second, the EU Database Directive, perhaps in reflex to the U.S. Supreme Court decision, does grant to the manufacturer of a database *sui generis* rights that vest in a database without regard to the innovation or originality required under U.S. copyright law.[103] Those rights are similar to many rights vested in owners of physical, tangible properties, including the ability to prohibit extraction or use of the data without suitable agreement.[104] Third, privacy and data protection laws conspicuously omit any direct references to "ownership" of PII; instead, there is a focus on the controls and limitations a data subject may exercise and/or negotiate through consent mechanisms.[105] Finally, in Japan, data is not subject to ownership under the Civil Code and, unless copyright, trade secret, or other legal statutes directly apply, data may be freely used.[106]

---

[102] *See* Feist Publ'ns, Inc. v. Rural Telephone Serv. Co., 499 U.S. 340, 363 (1991); *see also* Assessment Techs. v. Wiredata, 350 F.3rd 640, 644 (7th Cir. 2003) ("A work that merely copies uncopyrighted material is wholly unoriginal and the making of such a work is therefore not an infringement of copyright."). For an excellent perspective on the impact of the *Feist* decision, *see generally* Craig Joyce & Tyler T. Ochoa, *Reach Out and Touch Someone: Reflections on the 25th Anniversary of* Feist Publications, Inc. v. Rural Telephone Service Co., 54 HOUS. L. REV. 257 (2016–2017).

[103] Directive 96/9/EC, of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, 1996 O.J. (L 77/20), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996L0009.

[104] *See generally Protection of Databases*, EUROPEAN COMM'N (June 7, 2016), http://ec.europa.eu/internal_market/copyright/prot-databases/index_en.htm (containing links to several useful, detailed analyses of the Directive and its subsequent implementation).

[105] *See, generally,* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf; Privacy Regulation 2013 under the Privacy Act 1988 (Australia), available at https://www.legislation.gov.au/Details/F2018C00011; and the Fair Credit Reporting Act, 15 U.S.C. § 168 (regulating, in part, the privacy of personal financial information).

[106] *See supra* notes 36–55 and accompanying discussion.

III. PROPERTY RIGHTS IN DATA — ACADEMIC REVIEW

In preparing this article, we sought to identify existing scholarship on proposing property rights for all data. Our purpose was not to exhaustively account for all analyses; instead, we were investigating whether the two fundamental principles on which our proposal rests (as presented in Part V *infra.*) have been previously considered. Those two principles are that a) data is physical, capable of being governed by property rights systems comparable to those in place as part of the global legal infrastructure,[107] and b) control of data, as already expressed in formal commercial statutes and international model laws, could be the basis on which property rights may be asserted and transferred.[108]

Our research did not uncover any considerations of those principles. But the concept of applying property rights to personal information has been vigorously debated and analyzed. In addition, recent work, particularly in Europe, is advocating property rights for industrial data. These are useful to highlight, if only to emphasize that the functional questions of *how* to assert, perfect, and govern property rights in digital information have not been addressed.

A. Personal Information and Data Subjects

Global legal standards for protecting personal information evolved with considerable speed. Today, across most developed economies, data subjects have rights—expressed in constitutions, directives, statutes, regulations, and judicial decisions—to regulate how their personal information, once collected, can be used, processed, or distributed.

As a general matter, the pivot point at which those rights are to be expressed is the mechanism for notice and consent. In those terms and conditions, most of the rights are described in detail, particularly when the rights differ from the statutory default rules. Certain additional rights, including the right to correct fictional data (which includes inaccurate statements of data purported to be factual data) and to remove the availability of specific personal information from databases or published resources (i.e., the right to be forgotten) also have been described in formal regulations. Of course, the EU's framework, updated by the GDPR, contrasts dramatically with the industry-specific regulatory approach in the United States.[109]

---

[107] *See infra* Part IV.

[108] *See infra* Part V.

[109] *See* Directive 96/9/EC *supra* note 103; *see generally* ALAN CHARLES RAUL, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 268 (2014), *available at* https://www.sidley.com/-/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-

1. American Scholarship

In the evolution of privacy laws, there were several detailed academic explorations of whether explicit property rights should be granted to data subjects with regard to their personal information, notably in U.S. literature.[110] Alan Westin proposed that personal information should be formally recognized as an object of property rights in the late 1960s.[111] The issue continues to be analyzed into the current decade and five more recent works are worth highlighting.

Professors Nimmer and Krauthaus asserted that the notion of privacy in the United States was first shaped and framed by an article by Warren and Brandeis published in 1890.[112] They concluded that, from that early point, privacy analysis in the United States abandoned any notion of being grounded in property law concepts. Instead, the expression of rights was based in tort (i.e., liability). A violation of an individual's rights entitled them to seek compensation because their ability to assert personal control had been abused, in the same manner that a corporation is presumed to have control of their trade secrets which, if abused, entitle them to seek recourse under tort law.

By contrast,

> Property rights in information focus on identifying the right of a company or individual to control disclosure, use, alternation and copying of designated information. The resulting bundle of rights and limits comprises a statement of what property exists in information . . . . A property analysis speaks in terms of transferable assets and fixed zones of legally enforceable control, rather than the type of

---

states/fileattachment/united-states.pdf (summarizing the diverse regulations and enforcement approaches in the United States).

[110] The American Bar Association Section of Science and Technology Law has established a Data Property Rights Committee. *See Section of Science & Technology Law: Data Property Rights Committee*, AM. BAR ASS'N, http://apps.americanbar.org/dch/committee.cfm?com=ST207055 (last visited Aug. 5, 2017). As part of their work, the Committee maintains an outstanding inventory of legal materials relevant to evaluating the evolution and debate regarding the exercise of property rights in data. *See* AM. BAR ASS'N, COMMITTEE SUMMARY OF ARTICLES ON THE LAW OF PERSONAL DATA (2014), *available at* https://www.americanbar.org/content/dam/aba/administrative/science_technology/2014_data_prop_rights.pdf.authcheckdam.

[111] ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

[112] Raymond T. Nimmer & Patricia A. Krauthaus, *Information as Property Databases and Commercial Property*, 1 INT'L J. L. & INFO. TECH. 3, 30 (1993–1994) (citing Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)). Those outside the United States may be surprised that privacy considerations arose so early in American jurisprudence!

> continuously flexible balancing of interests and reliance on standards of reasonable behavior common in constitutional or tort law analyses."[113]

The distinction was elaborated on by Professors Lemley and Weiser:

> Traditionally, rights such as the ownership of real property are generally protected by injunctions, while tort and contract rights are enforced by means of compensatory damages. As famously explained by Calabresi and Melamed, these different remedial options represent alternatives for enforcing a legal entitlement—a property rule provides for an injunction and a liability rule provides for nonconsensual access in return for a payment of money damages.[114]

Professor Bergelson used this distinction to advocate that property rights were a suitable legal foundation for personal information in the United States.[115] She recommends certain rights be "inalienable," incapable of being foreclosed even if other rights for specific data have been transferred. She suggests those include rights to obtain records, demand corrections, and block or erase inaccurate information.[116] In doing so, she moves into offering a structure for property rights that is distinctive from those rights grounded in tort.

This distinction influenced the evolution of our proposal. To assert that a property rights system is suitable for all data has two implications. First, the existing legal structures for personal information (including the GDPR) need to be evaluated by asking whether there are any different notions of property rights now established. Quite simply, we do not see that to be the case. Instead, while the GDPR includes useful reforms responsive to new technologies, business models, and improving accountability, the fundamental structure is still expressive of a tort law framework in which vague or ambiguous standards must be applied within a variable larger context described by relevant circumstances and actions. The same is true in the United States.[117] Second, is there any explicit property rights or tort

---

[113] Nimmer & Krauthaus, *supra* note 112, at 5–7.

[114] Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783, 786 (2007) (citing Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972)).

[115] Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2005).

[116] *Id.* at 444 (citing Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) art. 12).

[117] Nimmer cites the Supreme Court's decision in *Feist Publ'ns, Inc.*, which reserves protection for databases determined to have sufficient originality in their

law construct established to protect industrial data beyond the portfolio of copyright and database laws? Again, we have concluded that is not the case. Professor Nimmer concurred, concluding that copyright laws are an unstable means of protecting distributed informational works, noting that protection relies on enforcing contractual obligations and technology controls.[118]

In 2011, Lund argued that an individual should have an "enforceable property right" over their own personal information.[119] Lund describes it as a "limited" property right, sufficient to allow individuals to enforce requests for retraction or correction of inaccurate personal information (therefore fictional data in our proposed classification).[120] Implicit is the burden on the data subject to prove the factual information asserted to be true is "readily verifiable."[121] The analysis fails to address how that right might be enforced across cloud-based services that cross national boundaries or other current complexities; illustrative examples of how the right might be exercised are built upon American actors seeking recourse in American courts under American judicial rules.[122]

Even earlier, in 1993, Laudon proposed information markets for personal information were entirely viable.[123] He envisioned the markets could be the only legal avenue for transferring personal information for secondary purposes; this idea is notable because it introduces structured governance for the administration of the property rights.[124] With his focus on personal information, Laudon offered:

---

design to overcome the general rule that assembled factual data is itself not protected. Nimmer & Krauthaus, *supra* note 112, at 15. This result is in contrast, of course, to the EU Database Directive, which grants explicit rights, but still conditions those rights on the level of effort invested in constructing and maintaining the database. *See generally* Directive 96/9/EC, *supra* note 103.

[118] Raymond T. Nimmer, *Information Wars and the Challenges of Content Protection in Digital Contexts*, 13 VAND. J. ENT. & TECH. L. 825, 826 (2011).

[119] Jamie Lund, *Property Rights to Information*, 10 NW. J. TECH. & INTELL. PROP. 1, *passim* (2011).

[120] *Id.* at 9.

[121] *Id. at 16.*

[122] *See generally id.* An earlier work by Professor Schwartz also advocated for these inalienable rights; the analysis is comparable, but dated by the evolutions in technology since its publication. *See generally* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).

[123] Kenneth C. Laudon, *Markets and Privacy* (Ctr. for Dig. Econ. Research, Working Paper No. 93-21, 1993), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1284878.

[124] *Id.* at 18. The debates and competing models between this type of centralized control proposed over 25 years ago and the decentralized administration envisioned

> No revolution in American property law is required to support national information markets. First, property law is quite flexible in recognizing value in a wide variety of tangible and intangible assets, including one's personal image. For instance, since the turn of the century courts have recognized the claims of celebrities to a property interest in their photographic image and the right of celebrities to seek compensation whenever their image is used for a commercial purpose. What is needed is the extension of a property interest to the digital data image of ordinary individuals.[125]

The surveyed American academic scholarship confirms that current U.S. law does not express a definitive right of ownership in any class of data, whether industrial data or PII. At the same time, there is nothing that appears to prevent legal reforms to establish those rights. What will be fascinating is whether the rights should be incorporated into federal law (such as copyright) or state laws (such as the laws for real property, goods, and various individual rights) with respect to the breach or unauthorized disclosure of PII. Our proposal does not restrict the mechanisms for implementation to any specific legislative body.

1. European Perspectives

Perhaps the most thorough European study on property rights in data was produced by Professor Purtova.[126] While limited to personal data, the analysis surveys the legal and pragmatic foundations of current EU laws on the scope of rights in data and how those rights might be governed. But, as stated by Purtova, "The key message this study hopes to convey is that it

---

by blockchain advocates will be fascinating; but neither model functions effectively if rights and obligations are not closely paired to, or coupled with, the information.

[125] *Id.* at 23. This concept is also capable of application to industrial data, consistent with our proposal *infra* Part V.

[126] *See generally* NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE (2011), *available at* https://pure.uvt.nl/portal/files/1312691/Purtova_property16-02-2011.pdf [hereinafter A EUROPEAN PERSPECTIVE]. For an abbreviated version of this work, *see* NADEZHDA PURTOVA, PROPERTY IN PERSONAL DATA: A EUROPEAN PERSPECTIVE ON THE INSTRUMENTALIST THEORY OF PROPERTISATION (2010), *available at* http://cadmus.eui.eu/bitstream/handle/1814/15124/10_Property_EN.pdf?sequence=1 [hereinafter A EUROPEAN PERSPECTIVE ON THE INSTRUMENTALIST THEORY OF PROPERTISATION]. In this paper, Purtova acknowledges that "so far only few European commentators have reflected on the possibility of propertisation." *Id.* at 3 (citing Corien Prins, *Property and Privacy: European Perspectives and the Commodification of our Identity*, *in* THE FUTURE OF THE PUBLIC DOMAIN, IDENTIFYING THE COMMONS IN INTERNATIONAL LAW (Lucie Guibault & P. Bernt Hugenholtz 2006)).

is impossible to give a simple 'yes' or 'no,' '1' or '0' answer to the questions on the possibilities of and need for propertisation."[127]

That conclusion is problematic for, in contrast to the more current calls in Europe for ownership principles to be adopted, there is no sense expressed by Purtova of why the notions of propertization were not embedded into the original and evolving states of EU data protection and privacy laws, nor any suggestion of how to navigate forward toward achieving that objective.

In early 2017, the Joint Research Centre of the European Commission issued a technical report on the economics of ownership, access and trade and digital data.[128] The report concludes that "the GDPR gives data subjects no full ownership rights, only certain specific rights"[129] While acknowledging the Database Directive "gives some limited property rights to data collectors," the report observes that there is a "wide area where ownership or residual rights are not legally specified, or incompletely specified."[130]

B. Property Rights in Data Other Than Personal Information

In the United States, both scholars and law reform organizations have considered whether property rights are appropriate for data other than personal information. Indeed, as summarized below, a formal model law was developed and approved for submission to the states for possible enactment. These materials were also considered.

In 2004, Professor Lipton contributed an important analysis of information property ownership, exploring the rights and obligations of owning information as property.[131] Her analysis emphasizes that information property rights must be balanced against important principles involving the preservation of information and ideas in the public domain, and balanced against competing private interests in the information and legitimate copyright and other intellectual property interests. In addition, she articulates how ownership also entails obligations, and uses metaphors and analogies from real property law as guidelines for constructing the

---

[127] A EUROPEAN PERSPECTIVE, *supra note* 126, at 12.

[128] Nestor Duch-Brown et al., *The Economics of Ownership, Access and Trade in Digital Data* (European Comm'n Joint Research Ctr. Working Paper 2017-01), *available at* https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf.

[129] *Id.* at 17.

[130] *Id.* at 18. The report references the extensive German materials and also explores in some depth the merit of clarifying rights to create proper incentives and summarizes other academic proposals on ownership within a European context. *See generally id.* at 18–20.

[131] Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FL. L. REV. 135 (2004).

obligations of data ownership.[132] Both of these facets are important to consider, of course, as more complete structures of ownership rights and responsibilities evolve. But our proposal focuses on more narrow questions: When and how can data ownership be established, and how can it be transferred in legitimate transactions? On these, Professor Lipton provided no guidance.

However, the concept of data ownership is not unfamiliar to American law. Beginning in the last decade of the twentieth century, in response to the absence of any treatment in the Uniform Commercial Code for software transactions, a model uniform law, known as the Uniform Computer Information Transactions Act (UCITA), was produced and adopted in 2002.[133] UCITA was comprehensive, going much further than just addressing software. The proposed Act offered a legislative framework to be adopted into state law that would also enable "computer information transactions" and "informational rights" in computer information. In doing so, UCITA offered enormous vision.

But the Act also presented the concept that software licenses could be structured with warranties of fitness and suitability, and other user-protective standards, concepts to which the software industry was strongly opposed. The result, to date, is that UCITA was only adopted in two states—Virginia and Maryland—and nearly all modern software agreements expressly disclaim the applicability of the law.[134]

C. Conclusions

Based on the preceding, we reached two conclusions that substantiate the urgency of the need to pursue a property rights scheme for data.

Our first conclusion is that, without exception, none of the prior analyses of whether a property rights scheme should be applied to digital information explicitly considered the vast quantities of data that are not personally identifiable information—that is, industrial data.[135] That seems

---

[132] *Id.* at 174–77.

[133] UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (UNIF. LAW COMM'N, Proposed Draft 2002), *available at* http://www.uniformlaws.org/shared/docs/computer_information_transactions/ucita_final_02.pdf.

[134] Detailed information about UCITA is available from the Uniform Law Commission. UNIFORM LAW COMMISSION, http://www.uniformlaws.org (last visited Jan. 5, 2018). One author of this paper, Jeffrey Ritter, was active in the drafting of UCITA for several years as a representative of the American Bar Association.

[135] The UCITA materials suggest that the full breadth of digital information was recognized by the drafting efforts, but the final version of the Act includes no characterizations that differentiate personal information and industrial data.

almost astounding, taking account of the volumes of data that are being produced and retained globally. Some public estimates project 2.5 quintillion bytes of data are created each day,[136] with total volumes growing at forty percent per year and the 2015 volumes projected to grow by fifty times by 2020.[137] Those expand to represent approximately forty-four zettabytes (1000^7 gigabytes) within less than three years.[138]

PII is only a small portion of the volumes of data that are created and retained each moment in each day of industrial operations. International shipping, fuel production, and business communications (such as electronic data interchange) produce enormous volumes entirely in support of business activities unrelated to individual persons. For example, business-to-business (B2B) electronic commerce transactions are projected to reach US$6.7 trillion by 2020, and each transaction produces data records entirely focused on the commercial transaction.[139]

Indeed, the apparent omission of any *industrial data* from prior deliberations on the suitability of a property rights scheme is surprising. While the regulation of PII is vital, the market confirms the wealth creation potential that can be extracted from industrial data. Indeed, the current and projected revenues from big data services are being realized without any substantive legal structure in place to define the information's ownership and attendant rights![140]

The second conclusion is that the academic deliberations, as well as the policy materials we reviewed, have not discussed in any manner the scientific consensus that digital information is, itself, physical. As examined

---

[136] *Every Day Big Data Statistics – 2.5 Quintillion Bytes Created Daily*, VCLOUD NEWS (Apr. 5, 2015), http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/.

[137] Michael de Waal-Montgomery, *World's Data Volume to Grow 40% Per Year & 50 Times By 200: Aureus*, E27 (Jan. 15, 2017), https://e27.co/worlds-data-volume-to-grow-40-per-year-50-times-by-2020-aureus-20150115-2/.

[138] Mikal Khoso, *How Much Data is Produced Every Day?*, NE. UNIV. (May 13, 2016), http://www.northeastern.edu/levelblog/2016/05/13/how-much-data-produced-every-day/; *see* Bernard Marr, *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, FORBES (Sept. 30, 2015, 2:19 AM), https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#b48f37017b1e.

[139] *B2B Ecommerce Market is Still Maturing*, EMARKETER (Aug. 8, 2016), https://www.emarketer.com/Article/B2B-Ecommerce-Market-Still-Maturing/1014311.

[140] In 2016, IDC projected that worldwide revenues for big data and business analytics will exceed $203 Billion in 2020. *Double-Digit Forecast for the Worldwide Big Data and Business Analytics Market Through 2020 Led by Banking and Manufacturing Investments*, INT'L DATA CORP. (Oct. 3, 2016), https://www.idc.com/getdoc.jsp?containerId=prUS41826116.

below in Part IV, that concept places much of the work during the last thirty years to adapt prior law to the nature of electronic commercial practices and digital commerce in a somewhat awkward position. If data is indeed physical, versus a form of intangible property, why has there been no legal construct modeled on well-developed property right systems for other types of physical assets?

No one seems to have asked or answered the question, "What is data?" There has been no inquiry as to the origin of data ("When does data begin to exist?"); no exposition on the classification schemes, data dictionaries, and other tools used to define and manage data ("What is this data in our possession?"); and, with few exceptions relating to anonymization of PII, no exploration of how data can be combined, transformed, processed, analyzed, and distilled into new combinations and output ("What can be done to data to make something new or create value in a transaction?").

These two conclusions are not meant to be critical of the prior literature; instead, they only serve to confirm that the proposals presented in Part V have not been previously considered. If there is not yet a clear, consensus-based agreement within the legal community on what data actually is—namely physical, tangible matter stored by electronic or similar means—how can a supportive, scalable, resilient legal construct be put into place that enables data-intensive transactions to prosper? To facilitate that consensus, we researched the simple question, "What is data?"

IV. THE PHYSICAL REALITY OF INFORMATION

In 1991, pursuing the potential for quantum computing, Rolf Landauer authored a landmark article titled *Information is Physical*.[141] That work was followed by several more papers in which Landauer presented a straight-forward point:

> Information is not an abstract entity but exists only through a physical representation, thus tying it to all the restrictions and possibilities of

[141] Rolf Landauer, *Information is Physical*, 44 PHYSICS TODAY 23–29 (1991). *See* John Mingers & Craig Standing, *What Is Information? Toward a Theory of Information as Objective and Veridical*, J. INFO. TECH., May 24, 2017, at 1("By objective, we mean that the information carried by signs and messages exists independently of its receivers or observers. The information carried by a sign exists even if the sign is not actually observed. By veridical, we mean that information must be true or correct in order to be information – information is truth-constituted. False information is not information, but misinformation or disinformation.").

> our real physical universe . . . information is inevitably inscribed in a physical medium.[142]

Landauer also stated convincingly

> Information is not a disembodied abstract entity; it is always tied to a physical representation . . . This ties the handling of information to all the possibilities and restrictions of our real physical world, its laws of physics and its storehouse of available parts.[143]

As summarized by Bawden and Robinson, the physical quality of information, and the idea that information is a physical constituent of the universe, are widely adopted within the scientific community.[144] The Foundational Questions Institute, a non-profit physics organization, has established a grant program to research the physics of information.[145] Considerable scientific research studies the physical attributes of information. From the earliest work of Claude Shannon in 1948 to set forth a definition of information offering a mathematical theory on information to ongoing research into information entropy, transmission velocities, data compression, and cryptography, the essential tangible state of information is a vital truth fueling continued advances in information technology.[146]

To this point in the evolution of regulating digital information, however, our review of the scholarship and legislative histories available to us suggests the physical nature of data (as defined above) has not been considered in deliberating on how to structure and apply the rule of law.[147]

---

[142] Rolf Landauer, *Information is a Physical Entity*, 263 PHYSICA A: STAT. MECHANICS AND ITS APPLICATIONS 63, 63–64 (1999).

[143] Rolf Landauer, *The Physical Nature of Information*, 217 PHYSICS LETTERS A 188, 188 (1996).

[144] *Id.*, and authorities cited therein.

[145] FOUNDATIONAL QUESTIONS INST., PROPOSAL REQUESTS, PHYSICS OF INFORMATION (2013), *available at* http://fqxi.org/data/documents/2013-Request-for-Proposals.pdf.

[146] *See* Roman Krzanowski, *Shannon's "Information" Revisited* (July 2016), *available at* https://www.researchgate.net/publication/304903301_Shannon_revisited. Claude Shannon's paper, *A Mathematical Theory of Communication*, available at http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf, is considered as the identifiable beginning of the field of information theory. *See* AFHAB ET. AL, INFORMATION THEORY AND THE DIGITAL REVOLUTION (2001), available at http://web.mit.edu/6.933/www/Fall2001/Shannon2.pdf.

[147] Our research has focused on academic research and publications available in the English and German languages. We fully acknowledge that scholarship or discussion connecting the physical quality of information to the regulation of data may exist in other languages. We welcome any suggestions on any additional research.

In contrast, the physical nature of data is beginning to influence other domains, notably information science as the basis for library operations.[148]

For our research purposes, *data, industrial data, personal information, factual data*, and *fictional data* each exist in tangible form. We make no distinction among different digital media and believe any such distinction would not be useful. What is important to accept is that the asset is tangible when recorded. Here are several examples to differentiate varying circumstances:

- In writing this paper, both authors are pressing keys that send electrical signals to the software application to create and display the image of each character. At the same time, the software application is storing the input; the data is the stored record. The result is the same, whether the storage is local to the laptop on which this paper is being composed, stored on a server to which a keyboard is connected within the college, or stored at a remote location maintained by a cloud services provider (such as a software company offering the application via the Internet). The record is *data*.
- The user's identity, and the usage behavior of that user with the application, may also be recorded as performance data relating to the user herself. Of course, based on the nature of that record, and its association with the user, *personal information* may also be created and stored.
- A sensor is a measuring device. It can be engineered to measure sound, frequencies, thermal energy, actions, or waves (of light or energy) as physical behavior. The sensor functions to convert the measured event into a record, an expression in digital form of the physical behavior that has been sensed. That expression, at the time the record is created, is now physical *data*. It is an example of *industrial data*. It exists, and the information contained in that record will be transmitted elsewhere or preserved. If the original data

---

[148] *See, e.g.*, David Bawden & Lyn Robinson, *"Deep Down Things": In What Ways is Information Physical, and Why Does it Matter for Information Science?*, 18 INFO. RES. 3 (2013), *available at* http://www.informationr.net/ir/18-3/colis/paperC03.html#.Wk_ont-nGHs.

is subsequently deleted, destroyed, or overwritten, it no longer exists as physical matter.[149]

- In complex automated business processes (including computational calculations), each step or element of the process is producing two outputs, each of which has unique physical status. First, the substantive output itself is created (e.g., the result of inputted data being calculated by an algorithm) and a record of that output is established. Second, the successful execution of the step or element also is recorded, usually in one or more logs, to create evidential support (i.e., factual data) the step or element was completed. The log data may or may not be associated with the specific output but provides an audit trail to the step's execution.[150] Each of these records would also be considered as *industrial data*.
- While pausing between drafts of this paper, an author went to an online entertainment provider to pay for and watch the latest episode of a popular fantasy fiction series. The browser, provider's website, and the author's bank all created records of the user's actions, most of which likely would include *personal information*. But, if observed and recorded without regard to identity (e.g., page selection and show previews viewed before log-in), those records are

[149] Of course, it is possible that copies of the data exist, and each copy is, itself, a separate physical asset. The law has long struggled with the ability of computers to create copies of records. *See generally* MICHAEL R. ARKFELD, ARKFELD ON ELECTRONIC DISCOVERY AND EVIDENCE (2005); Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1 (2009). For a British perspective, *see* INST. OF ADVANCED LEGAL STUDIES, ELECTRONIC EVIDENCE (Stephen Mason & Daniel Seng eds., 4th ed. 2017). In actuality, the full record, including all associated metadata, when encrypted and time-stamped, is physically unique. Recent technologies, such as blockchain-based ledgers, are overcoming the presumption that copies of specific data are indistinguishable. *See generally* EUROPEAN AGENCY FOR NETWORK AND INFO. TECH., DISTRIBUTED LEDGER TECHNOLOGY AND CYBERSECURITY (2017); Zach Church, *Blockchain Explained*, MIT SLOAN (May 25, 2017), http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/; Jonathan Hassel, *What is Blockchain and How Does it Work?*, CIO (Apr. 14, 2016, 3:48 AM), https://www.cio.com/article/3055847/security/what-is-blockchain-and-how-does-it-work.html.

[150] Business process management (BPM) software solutions and business process engineering languages (BPEL) are important tools used in the creation of these types of performance and event logs.

industrial data. The content of the episode would be *fictional data* (especially if dragons are involved!).

In viewing information as physical matter, and accepting that view as the foundation for a new way of thinking about property rights systems for data, the following observations can also be made. First, physical information can be very small. A single byte is sufficient to exist.[151] Advances in quantum computing are confirming that qubits also are now working in small, functioning computers.[152] Recognition of physical information as property does not require, in principle, any de minimis size requirement. That opens up all sorts of possibilities to enable our machines to track the existence and use of data with granularity that is not humanly possible. This transforms enforcement and compliance into behaviors that do not rely on human observation.

Second, classification of data is *not* derived solely from its actual content; the surrounding context (including the identity and role of the various actors, systems, applications, and functions each are performing) can affect how data is classified in order to apply advanced rules specific to a classification type. Unfortunately, with the exception of PII, no other formal classification methods exist around which rules regarding ownership, control, and use can be structured. Building those classification methods will be an important part of how the legal constructs for data evolve.

Finally, objective recognition of data as tangible matter, in whatever volume or size, opens the door to asking whether a) original creativity is required as a pre-condition to exercising legally recognized rights (such as those bestowed on copyright owners under U.S. law),[153] or b) whether a database creator has made sufficient investment in the database to be vested with *sui generis* database rights, as provided by the EU Database Directive.[154] Neither of those measures, as expressed in current laws, enable reliance on objective, automated mechanisms to establish ownership and the

---

[151] *See Byte,* ENCYCLOPAEDIA BRITANNICA, https://www.britannica.com/technology/byte (last visited Aug. 23, 2017) ("[A] byte [is] the basic unit of information in computer storage and processing. A byte consists of eight adjacent binary digits (bits), each of which consists of a 0 or 1.").

[152] *See* EVGENIY KIKTENKO ET AL., QUANTUM-SECURED BLOCKCHAIN (2017), *available at* https://arxiv.org/pdf/1705.09258.pdf.

[153] *See generally* Feist Publ'n Inc. v. Rural Tel. Serv. Co., 499 US 340 (1991); Assessment Techs. v. Wiredata, 350 F.3rd 640 (7th Cir. 2003); Craig Joyce & Tyler T. Ochoa, *Reach Out and Touch Someone: Reflections on the 25th Anniversary of* Feist Publications, Inc. v. Rural Telephone Service Co., 54 HOUS. L. REV. 257 (2016–2017).

[154] *See* Directive 96/9/EC, *supra* note 104, at Articles 7, et. seq.

subsequent exercise of the rights of ownership. This makes it difficult to imagine how the laws themselves will be capable of dynamic enforcement.

V. A PROPOSAL AND NEXT STEPS

Our proposal begins by answering the question, "When does data begin to exist?" We propose that data becomes real the moment it is recorded by electronic or digital means. At that point in time, something tangible exists that is new and different from the preceding moment in time. Data creation occurs through one of two methods—either a human user inputs instructions to create a data asset (such as pressure on a keyboard creating the letters of this paper in a digital format) or a machine executes a process that records new data of various classifications. The data may be a light impulse, an audio sound, a pixel within an image, or an entire digital photograph instantaneously captured and preserved. There is no necessity that the data itself be in perceivable form through the use of human senses; it is sufficient to have evidence the data exists (in other words, data about data that confirms its existence and state).[155] In order for the data to become subject to property rights, several other questions immediately become important to resolve:

- How is the data to be classified? What data about the data and surrounding context are required to calculate and establish the classification?
- When do the rights of ownership attach to the data? Does the answer vary based on how the data may be classified?
- What controls or constraints are relevant to the data based on its classification? How may those be effectively exercised?
- What rights or uses does ownership entitle an owner to exercise?

In contrast to existing legal standards associated with copyright and databases (through which the rights of parties in the content are based on subjective measures of creativity, originality or level of effort), we propose that the answers to each of the preceding questions must be capable of being computationally calculated in objective reliance upon sensor records and transactional data stored in metadata and associated logs. This is not such a

---

[155] *See* U.C.C. § 9-102(a)(70) (AM. LAW INST. & UNIF. LAW COMM'N 2010). The notion of "perceivable form" was introduced in the United States Uniform Commercial Code definition of "record," developed during the 1990's in response to accelerating electronic commercial practices. *See, e.g.,* U.C.C. § 1-201(b)(31) and U.C.C. § 2-201(b)(31). For a perspective on the considerations and dynamics involved in introducing the new definitions, *see* Patricia Brumfield Fry, *X Marks the Spot: New Technologies Compel New Concepts in Commercial Law*, 26 Loy. L.A. L. Rev. 607 (1993). The definition of "data," introduced *supra* Part I, allows the perception of the existence of data to be made by a machine.

radical notion; many laws and regulations are constructed around metrics generated by automated technologies (e.g., speed limits, particulate levels in factory emissions, concentration limits on certain chemicals and fertilizers, etc.). Our proposal extends that concept into the operation of complex information systems in which the rules of ownership-and rights-are electronically expressed and enforced. The rules will be enforceable based on measurements of behavior and actions taken (and not taken) within the systems and processes themselves.

Through various existing and foreseeable technologies, systems can be envisioned in which a) the data owner's property rights may attach to data at very early moments in the data's lifecycle, b) data classifications can be bound to the data (along with associated factual information regarding parties entitled to exercise constraints on downstream uses of a data asset, such as personal identity), and c) controls and constraints can be automatically applied and enforced. Across the vastness of cyberspace, both in the present and into the future, no other mechanisms are rational to consider. Stated differently, compliance and rights must become functions that are derived from mathematical calculations. To achieve that outcome, this article's proposed construct serves as a platform on which to build.

A. Attaching Ownership to Data

Once data exists as physical matter, the next question is, "When do the rights of ownership attach to the data?" As noted earlier, the rule of law for personal information does not provide any clear benchmark of when ownership does or does not attach to the information itself.[156] Yet, as described in Part II, there are growing international calls for ownership rights to be clearly defined for all data, including industrial data or personal information, in large part to facilitate increased transactional volume and revenue in data as the asset of the deals, whether for licensing, aggregation into data lakes, fostering innovation, or other analytical or creative purposes.

But, in attaching ownership rights to data, other ancillary issues immediately arise and must be considered: How can evidence of the attachment of ownership rights be recorded? What does that evidence consist of (as transactional data about the event of attaching ownership)? Does the ownership attach merely to the primary data (such as an entry in a database or the recorded output of a process) or does ownership also attach to the related event and process logs and associated transactional information (i.e., the provenance record for the primary data)? Does ownership include any data that was created in order to support the

[156] *See supra* Part III A.

classification of data which, in turn, attaches certain rights, controls, and constraints (such as those of a data subject relating to their PII)?

We propose that these questions, and the foundation for calculating when and how data rights attach, can be answered by modeling and extrapolating from existing legal systems for governing transactions tangible assets, including goods, real property, and documents of legal significance, such as chattel paper. In each of these systems, the same questions have been previously considered and robust, mature legal frameworks and commercial systems have evolved. In each, once ownership is established, ownership and other derivative rights can be transferred between separate parties in one or a series of separate transactions. A quick survey of current commercial practices confirms that transactions involving data are not inherently unique or different, except for the absence of the necessary predicate of defining how ownership attaches. We can extract some important generalized principles from these complex legal systems.

Most commercial legal systems precisely define "goods," and include agricultural commodities and manufactured products in those definitions. For example, in the U.S. Uniform Commercial Code (UCC), goods must be "existing, identified, and movable at the time they are identified, in order for any interest in them to pass."[157] Goods also includes the unborn young of animals, growing crops and other identified things that can be severed from real estate; however it is the tangible born animal or harvested crop that becomes the asset around which a transaction is built.[158]

- For data, the requirement the data "exists" is entirely suitable. All data is a record of an action taken, created and preserved in physical form, descriptive of an event, an action, a calculation, or the performance of a process. Data must exist to be capable of being owned.
- For transactions in data, there must be "identification." Data identification requires both classification (what type of data is it?) and description, sufficient to enable a transaction to be specific to the relevant data. Within computer technology, that can require a careful balance—descriptive identifications cannot be insufficient nor so overly detailed as to inhibit efficient processing.

---

[157] U.C.C. § 2-105(1)–(2) (AM. LAW INST. & UNIF. LAW COMM'N 2002).

[158] *Cf. United Nations Convention on Contracts for the International Sale of Goods*, UNCITRAL (Apr. 11, 1980), http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods/1980CISG.html (providing no explicit definition of "goods," but contemplating contracts for the supply of goods to be manufactured or produced).

- By contrast, for transactions in data, legal reforms to enable electronic commercial practices in which electronic assets are the focus of the transaction have confirmed that data need not be "movable"; as discussed below, a data transaction can be fully performed through a transfer of 'control."[159]

With real property, most developed and developing economies have created rule systems through which ownership is defined based on physical descriptions of the real estate, and the records of ownership are the related contracts describing the transfer of title between buyer and seller, such as a deed. The integrity of those contracts, and the validity and priority of ownership, are confirmed by recordings of those contracts filed in public offices that serve as custodians for those records.[160] Ownership attaches through a specific legal process of formal transfer, and the priority of competing claims of ownership is established by considering the contracts and public records.

- For existing and foreseeable data transactions, as noted above by the "identification" requirement for goods, the subject of the transaction will also require description. It is now apparent that data descriptions must also include some means to either a) identify the system(s) on which the data is located (remember, if data is physical, it is always some "where"), or b) uniquely identify and describe the data to enable its location to be irrelevant, provided the other descriptive information elements can be proven to be accurate and connected to the subject data itself. While conventional discussions suggest data files can be duplicated, when properly enveloped or associated with related metadata and provenance, and bundled by suitable encryption or other controls, any data file can, in fact, be unique and incapable of perfect duplication.[161]
- While data title registries, particularly by public authorities, do not currently exist beyond those

---

[159] *Infra* notes 175-186.

[160] *See generally* RESTATEMENT (THIRD) OF PROPERTY (AM. LAW INST. 2001); *see also* HARPUM ET AL., THE LAW OF REAL PROPERTY (8th ed. 2012).

[161] *See generally infra* Part V of this article. New developments in blockchain, zero-knowledge proofs, and quantum cryptography suggest the uniqueness of a data asset are entirely foreseeable; however, the supporting detail in this article is beyond the scope of this article.

> associated with copyrighted materials, patents, and trade and service marks, the idea has, in fact, been proposed.[162] In many respects, blockchain functions as a similar registry, creating a cryptographically secure record of the contents, submitting party, and time-stamps for any data asset placed onto a blockchain.[163]

For documents with legal value, such as chattel paper, banks and financial service interests began in the 1990s to consider how ownership of legal documents such as chattel paper might be established and transferred if the legal documents were, themselves, electronic records. Prior to that time and continuing into the present day, the ownership of physical chattel paper was defined by the information appearing on the face of the chattel paper itself and, if offered as collateral to secure loans, by formal filings of notices.

A series of amendments to the UCC (and, in turn, U.S. federal statutes) provided the foundation for ownership and transfer of their electronic equivalents (including the rights to enforce the promises represented by chattel paper). In summary, those amendments and statutes offer the following key concepts, each of which support our proposal to apply property right systems to digital information.

First, "Record" is defined as "information that is inscribed on a tangible medium or which is stored in an electronic medium or other medium and is retrievable in perceivable form."[164] Next, "electronic chattel paper" is defined to consist of "chattel paper evidenced by a record . . . consisting of information stored in an electronic medium."[165] Together, these defined terms enabled the digital information to be classified and, in so doing, allowed rules for establishing and maintaining control of

---

[162] *See, e.g.*, Andreas Wiebe, *Protection of Industrial Data—A New Property Right for the Digital Economy?*, 12 J. INTELL. PROP. LAW & PRAC. 62 (2016); WOLFGANG KERBER, "INDUSTRIAL DATA RIGHT" AND INNOVATION? (2016), *available at* http://www.grur.org/uploads/tx_meeting/04_Kerber_GRUR_1506 2016_02_17.pdf.

[163] *See generally supra* note 145. General explanations of blockchain are abundantly available, and many current implementations are emphasizing the integrity of the records and the resulting "distributed ledger" as equivalent to the registry functions of government offices or other central authorities.

[164] U.C.C. § 9-102(a)(70) (AM. LAW INST. & UNIF. LAW COMM'N 2010). This definition was constructed to assure the equivalence of information stored in electronic media to tangible paper documents. This definition did not prescribe any defined structure, volume, or minimum requirements for a record, which enabled many requirements for records set forth in the U.C.C. to be satisfied by electronic files, whether or not relating to the chattel paper.

[165] U.C.C. § 9-102(a)(31) (AM. LAW INST. & UNIF. LAW COMM'N 2010). This definition emphasized it was the stored electronic record of the chattel paper's existence that became the focus of the following steps.

electronic chattel paper to be crafted and applied. These rules specified that a secured party (with a security interest in the chattel paper) "has control of electronic chattel paper if a system employed for evidencing the transfer of interests in the chattel paper reliably establishes the secured party as the person to which the chattel paper was assigned."[166] In turn, those rights of a secured party can be transferred to other secured parties by transferring the rights of control over the electronic chattel paper.

The integrated process of establishing control and enabling transfers has been expanded to enable transactions in other electronic transferable records, documents, or instruments. Building on the UCC reforms, U.S. federal law was enacted in 2000 to enable electronic promissory notes for loans secured by real property to become transferable records, including those executed using electronic signatures.[167] Then, in 2017, these concepts were integrated into a Model Law on Electronic Transferable Records was formally approved by the United Nations Commission on International Trade Law (UNCITRAL).[168]

A distinctive feature of this UN Model Law is the definition of "electronic record" and its specific focus on metadata and similar information. "'Electronic record' means information generated, communicated, received or stored by electronic means, including, where appropriate, all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not."[169] This view of an electronic record highlights that metadata and other log data (if logically associated with or otherwise linked together to become part of the record) need not be generated at the

---

[166] U.C.C. § 9-105(a) (AM. LAW INST. & UNIF. LAW COMM'N 2010). The reliability test of 9-105(a) was one for which additional guidance is provided as to the specific facts that can be demonstrated to evidence the existence of control. *See* U.C.C. § 9-105(b) (AM. LAW INST. & UNIF. LAW COMM'N 2010). These are further discussed in the text accompanying *infra* notes 175-186. Co-author Jeffrey Ritter was substantially involved in the drafting of the revisions described here, serving as an advisor for the American Bar Association to the drafting committee for these revisions during much of the reform process.

[167] The Electronic Signatures in Global and National Commerce, also known as the 'E-Sign Act', Pub. L. No. 106–229, tit. II, § 201, 114 Stat. 473 (2000).

[168] For the final text of the Model Law, *see* U.N. COMM'N INT'L TRADE, UNCITRAL MODEL LAW ON ELECTRONIC TRANSFERABLE RECORDS, U.N. Doc. V.17-0543, U.N. Sales No. E.17.V.5 (2017), *available at* http://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf [hereinafter "MODEL LAW"]; *see also UN Commission on International Trade Law Adopts the UNCITRAL Model Law on Electronic Transferable Records*, U.N. INFO. SERV. (July 17, 2017), http://www.unis.unvienna.org/unis/en/pressrels/2017/unisl251.html.

[169] MODEL LAW, *supra* note 168, at Art. 2.

same time as the primary content, but may be generated either before or after. This concept is, in our opinion, quite constructive toward a more formal property rights system and enables how data will be classified and how the rules for managing that information can be identified to be associated with a specific electronic record by automated means. In other words, the records of ownership and control can exist independent of the asset itself (which is no different than a land registry or the filing systems used to give notice of security interests).

The UNCITRAL Model Law also addresses the notion of what may be an "original," noting in their work papers that electronic transferable records are meant, by their own nature, to circulate.[170] The Model Law achieves the goal of preventing multiple claims of originality by relying on concepts of "singularity" and "control" that allow both the person entitled to enforce the note (or similar electronic asset) and the object of control to be identified in a unique, secure manner.[171]

This Model Law (as well as the U.S. enactments) articulates attributes and processes that can apply to any data; the definition of "electronic record" is not limited to the digital equivalents of transferable documents or instruments.[172] First, these laws anticipate that markets will want to achieve transferability of the digital versions of physical transferable documents; indeed Article 10 of the Model Law defines the conditions with which an electronic record satisfies legal requirements for a physical transferable document or instrument.[173] Article 17 expressly allows an electronic transferable record to replace a physical document "if a reliable method for the change of medium is used."[174] Current digital practices, and the calls for data ownership, emphasize that data has become something for which the value is increased by its transferability and utility in multiple environments, systems, and contexts. As evidenced by many big data analytics developments, data in any volume is capable of being licensed, transferred, and divided into downstream revenue opportunities in

---

[170] Note by the Secretariat, Draft Model Law on Electronic Transferable Records, A/CN.9/WG.IV/WP.139, at para. 81–82, available at http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html. For additional working documents tracing the evolution of the Model Law, *see Working Group IV*, UNCITRAL, http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html (last visited Jan. 6, 2018).

[171] Note by the Secretariat, *supra* note 170, at para. 82.

[172] MODEL LAW, *supra* note 168, at Art. 2.

[173] *Id.* at Art. 10. Art. 7(1) provides further reinforcement that "[a]n electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form." *Id.* at Art. 7(1).

[174] *Id.* at Art. 17.

the same manner as other legally valued electronic records, all while ownership continues to be claimed by the original custodian.

Second, the laws anticipate that transferability of unique data assets (where only one party can have enforceable rights with respect to electronic chattel paper) can be achieved by defined processes that transfer control of the digital asset versus transfer of the physical asset, for which many existing commercial laws exist.[175] A property rights system for electronic information could effectively leverage the legal structures that have already been developed for electronic records and how control is used as a mechanism for enabling market-based transactions. A single byte of data, once recorded on any electronic medium, is merely a smaller electronic asset for which ownership could be established.

B. Attaching Ownership – The Exercise of Control

We propose that the rights of ownership for specific data attach at that point in time and process at which an entity establishes *control* of the data. This concept, which largely tracks the reforms for electronic chattel paper and transferable records, requires elaboration (which follows below), but the principle both leverages and contrasts against some established legal principles in copyright and database law in two fundamental ways.

First, there is no requirement that the data be complete, sensible, or a finished product. This is consistent with copyright law: the related rights do not require a formal notice or registration and copyright attaches at the time of creation, even to works in process.[176] So, too, can rights of ownership attach to any data at the time of its creation, even if the record is itself partial or incomplete.

---

[175] For example, in the Uniform Commercial Code enacted among the states, Articles 3 (Negotiable Instruments) (defining the rights of holders and holders in due course), 4 (Bank Deposits and Collections) (defining the rights of holders of check items), 5 (Letters of Credit) (defining the rights of presenters and issuers of letters of credit), 7 (Documents of Title) (defining the rights relating to the negotiation of warehouse receipts and bills of lading) and 8 (Investment Securities) (defining the rights of those in possession of security certificates) all directly regulate the processes by which physical documents can be transferred as well as the legal consequences. U.C.C. §§ 1-101 to 9-709 (AM. LAW INST. & UNIF. LAW COMM'N 2012).

[176] *See* 17 U.S.C. § 101 (2010) (defining a work as "fixed" when it is captured in a sufficiently permanent medium that the work can be perceived, reproduced, or communicated for more than a short time). This notion is comparable to data being created and controlled; there must be some basis of permanency to the data itself. For example, data that consists of log inputs which, within a few milliseconds, are forever overwritten and destroyed would not be within the scope of the proposal.

Second, there is no expectation here that creativity or original work of authorship, or any level of effort of an undefined degree, is required. In this respect, data ownership is comparable to the EU database protection and not consistent with the U.S. view that mere statements of facts are not copyrightable.[177] What matters is the physical existence of the data and the establishment of initial control.

C. Establishing Control

Common law systems favor possession and physical control of goods or real property as factual considerations from which to begin evaluating ownership and the lawful exercise of the rights of ownership.[178] But, for electronic commerce and for data as property, the UN Model Law and U.S. legal reforms offer *control* as an equivalent indicium from which those rights may be exercised. What are those indicia? If we merely substitute a) "a person" (which may be a corporation or individual) for "secured party," and b) "data" for either "electronic chattel paper" or "electronic transferable record," the remaining statutory language might be further modified to read as follows:[179]

> A person owns data when the person establishes control of the data.
>
> A person has control of data if a system employed for recording and evidencing the transfer of interests in the data reliably establishes the person as the owner or the person to which control was assigned.

---

[177] *See id.*; *see also* Feist Publ'n Inc. v. Rural Tel. Serv. Co., 499 US 340 (1991); Assessment Techs. v. Wiredata, 350 F.3rd 640 (7th Cir. 2003); Craig Joyce & Tyler T. Ochoa, *Reach Out and Touch Someone: Reflections on the 25th Anniversary of* Feist Publications, Inc. v. Rural Telephone Service Co., 54 HOUS. L. REV. 257 (2016–2017). As discussed earlier, data ownership systems must be capable of being automatically operated, and the subjective standards that characterize copyright and database legal protection are not functional across complex information systems.

[178] *See* JOHN E. CRIBBET & CORWIN W. JOHNSON, PRINCIPLES OF THE LAW OF PROPERTY 12–13 (1962); In re Garza, 984 S.W.2d 344, 347 (Tex. App. 1998) (citing RALPH E. BOYER, SURVEY OF THE LAW OF PROPERTY 679–80 (3rd ed. 1981)).

[179] The language is modified from U.C.C. § 9-105 (AM. LAW INST. & UNIF. LAW COMM'N 2010). Similar language exists in the E-Sign Federal law and the UNCITRAL MODEL LAW with minor variations not directly relevant to the proposal at this stage. *See* MODEL LAW, *supra* note 168, at Art. 12 (emphasizing reliability, data integrity, preventing unauthorized access, security, audit, and third-party confirmation of reliability).

> A system satisfies [the definition of control], and a person is deemed to have control of a data record,[180] if related records are created and stored in such a manner that:
>
> (1) a single authoritative copy of the data exists which is unique, identifiable, and, except as provided below, unalterable;
>
> (2) the authoritative copy identifies the owner as the owner of the data;
>
> (3) the authoritative copy is communicated to and maintained by the owner or its designated custodian;
>
> (4) copies or amendments that add or change an identified transferee of the authoritative copy can be made only with the consent or prior approval of the owner;
>
> (5) each copy of the authoritative copy, and any copy of a copy, is readily identifiable as a copy that is not the authoritative copy; and
>
> (6) any amendment of the authoritative copy is readily identifiable as authorized or unauthorized.

Under this set of rules, more is needed than mere data creation in order for ownership rights to *attach* in a manner that could be legally defensible. There must be a system used that enables the owner to record the fact that their control of that data has been established and in a manner that satisfies how control is defined. The Model Law provides that a transfer of "control" for electronic transferable records is legally sufficient to meet any requirement for, or permitted transfer of, physical possession of transferable documents.[181]

For self-contained systems currently used inside a company or organization, many different commercial information governance and records management systems might be fully satisfactory. But more is needed across the complexity of today's IT environments, which have systems of systems through which data passes across multiple firewalls and system perimeters. Here are some examples:

- A company outsources its business software applications to use a cloud software-as-a-service provider. The data, when keyed in during normal user activity, is immediately stored on the service provider's servers or, perhaps, transferred to the servers of a subcontractor to the service provider. In these circumstances, the contract(s) become vital tools

---

[180] *See* 15 U.S.C. § 7021(c) (2000).
[181] MODEL LAW, *supra* note 168, at Art. 11.

for confirming ownership and control of the data by the licensee company.

- Many big data licensing deals involve transferring copies of selected data to third-party analytics firms. If those copies might be recorded by a system that tracks control, as contemplated above, the rights of the analysts, as well as the original corporate contributor of the data, could be more rationally differentiated and administered.
- While the source data inputted might have multiple originating owners that have transferred control of copies to the analytics firm, the output of the analytics is new data, created by the analytics firm. Now, all parties (contributors of original copies, the analytics firm, and their customers for the output) must articulate their respective rights in that output. Contracts are the governance and enforcement vehicles, but the identification and exercise of rights with respect to the output data pursuant to the agreement can be automated into the relevant control systems.

The Model Law introduces an intriguing path forward in determining how the sufficiency of systems delivering control are to be evaluated. In seven different articles, the legal standard by which to measure a specific method is one of reliability.[182] In support of those references, Article 12 articulates a general reliability standard, directing that a method shall be "as reliable as appropriate for the fulfilment of the function for which the method is being used, in the light of all relevant circumstances."[183] This standard, of course, like many common law rules, invites the potential for nearly endless debates as to whether particular methods employed for a specific transaction were "reliable." But Article 12 goes further, identifying an illustrative listing of circumstances that may be relevant.[184]

---

[182] *Id.* at Arts. 9–17.

[183] *Id.* at Art. 12(a).

[184] The list includes:

(i) Any operational rules relevant to the assessment of reliability; (ii) The assurance of data integrity; (iii) The ability to prevent unauthorized access to and use of the system; (iv) The security of hardware and software; (v) The regularity and extent of audit by an independent body; (vi) The existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method; (vii) Any applicable industry standard.

Id.; *see also id.* at Art. 12 cmt. 122–39.

The practical effect of this listing is to create a template against which any method must be designed. In other words, any method that does not proactively incorporate operational rules for assessing reliability, assuring data integrity, preventing unauthorized access, securing hardware and software, requiring regular and extensive audits, securing accreditation, and complying with applicable industry standards is easily challenged as being insufficiently reliable. Looking forward, our proposal for how to expand the concepts of control into enabling new markets should surely build upon, and be measured against, the same template elements to improve the likelihood of early successes.

Article 12 offers another alternative. Under 12(b), a method can be reliable if "proven in fact to have fulfilled the function by itself or together with further evidence." As explained in the Explanatory Note, this provision is similar to one used for demonstrating the functional equivalence of electronic signatures to physical signatures under the Electronic Communications Convention.[185] If a method can be proven to have worked as intended, reliability need not be the basis of frivolous litigation.[186] This concept is also important, particularly if market participants commit to, and actively use, a specific method to maintain control across many different transactions; their prior conduct confirms the reliability of the systems, foreclosing further disputes.

After years of negotiation at the United Nations, the Model Law offers a governance structure that is well-suited to enable how ownership in data might be defined and ownership rights attached (and subsequently transferred). As well, those derivative rights can themselves be expressed in metadata or other information "logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not."[187]

The finalization of the Model Law delivers a strong, international platform upon which our proposed model can expand. In other words, the proposal here is intended to leverage and enable agreements that connect commercial transactions working across multiple national boundaries. The foundation is already in place to do so as a result of the Model Law.

Formulating a legal structure that is scalable and extensible for data on a global basis into the foreseeable future certainly will require many

---

[185] *Id.* at Art. 12 cmt. 136–137. *See* U.N. COMM'N INT'L TRADE L., UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS, U.N. Doc. V.06-57452, U.N. Sales No. E.07.V.2 (Jan. 2007), *available at* http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf.

[186] MODEL LAW, *supra* note 168, at Art. 12.

[187] *See* MODEL LAW, *supra* note 168, at Art. 2 (defining "electronic record").

nuances and adjustments. The reliability criteria of Article 12(b) in the Model Law suggest a good inventory of the work ahead. Our proposal, however, remains grounded in the simple truths that a) data is physical matter, and b) legal reforms at the international level have already been formulated that migrate traditional legal rules based on physical records into the more electronically enabled commercial practices of the present. Leveraging those rules to advance a property rights system applicable to all data *is* possible.

D. Reconciling Existing Privacy Laws

As noted earlier, privacy laws have often been the intense focus of academic debate as to whether property rights systems were appropriate for personal information. In our analysis of the related scholarship, the view often was one of either/or—personal information must be governed by either a property rights system or a torts-based system (with the latter being viewed as the prevailing model). We believe there is a way in which the rights of data subjects can be accommodated within the larger framework of a property rights system for all data.

As noted earlier, to assert control, data must be both identified and classified. As a practical matter, those actions are now entirely automated. But once data is classified as PII, the owner can still be immediately subject to the same constraints imposed by current privacy laws on how the PII may be used and transferred. Indeed, that is no different than current legal systems, other than that the ownership of the PII by the collecting entity (i.e., controller) is now explicit, rather than inferred.

Defining ownership does not derogate from the ability of data subjects to still exercise tort-based rights and remedies if controllers or processors violate the terms of consents that are given. Concepts of clear ownership are useful, as well, to the negotiating position of a data subject; if they wish to explicitly retain ownership of the identifiable data relating to them, that can be an express topic in the negotiations which notices and consents under current law theoretically enable (as well as the possible consideration payable to the data subject for the transfer of ownership to occur).[188]

---

[188] *See, e.g.*, WORLD ECON. FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE (2013), *available at* http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf; Cassandra Liem & Georgios Petropoulos, *The Economic Value of Personal Data for Online Platforms, Firms, and Consumers*, LSE BUS. REV. (Jan. 19, 2016), http://blogs.lse.ac.uk/businessreview/2016/01/19/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/ (reporting on the calculation of advertising revenues per user (ARPU) reported by major online providers such as Google and Facebook); Jeff Desjardins, *How Much is Your*

For example, from this point forward, many electronic consumer products, including automobiles, will become data collection devices.[189] For each, we envision that a property rights framework allows explicit recognition of a) the product itself (such as the car), and b) the future data streams (both of industrial data and personal information) the product will produce. The sensor networks within cars and trucks certainly can associate some data to the operator of the vehicle, which becomes personal information subject to normal law. But much of the data those networks will collect has primary industrial value—predicting maintenance repair needs, improving innovation, identifying time to failure for specific components—which is valuable to car manufacturers, component suppliers, and service networks irrespective of the identity of the human operator. How is ownership of that future data defined? In Germany, the ministry of transport and digitalization defines the ownership of data created by automobiles as follows:

> Die Verfügungsrechte an Daten sollen demjenigen zugewiesen warden, auf den die Erstellung der Daten zurückgeht. Damit gilt im Grundsatz: Die Daten und damit verbundene Rechten gehören den Menschen – bei Fahrzeugdaten etwa dem Halter,[190] der das Fahrzeug erworben hat.[191]

Personal Data Worth?, VISUAL CAPITALIST (Dec. 12, 2016, 11:30 AM), http://www.visualcapitalist.com/much-personal-data-worth/ (reporting nine key data brokers realized $426 million in annual revenues, as of 2012). Significant research that has been conducted on the economic value of PII to data subjects, both amounts payable to secure clear rights of use, as well as the downstream revenues PII generates from which data subjects are normally excluded in the marketplace. For an interesting calculator used to calculate the value of an individual's data, *see* Emily Steel et al., *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013), http://ig.ft.com/how-much-is-your-personal-data-worth/. In contrast, for industrial data, the "monetization" of data in commerce is driving entirely new innovations in how accounting practices (and others) measure and express the economic worth of information. *See* Hedge, *supra* note 9.

[189] *See* Matthew Wilson, *BMW and IBM Team Up for Cloud-Connected CarData Network*, IBM (June 16, 2017), https://www.ibm.com/blogs/cloud-computing/2017/06/bmw-ibm-cloud-cardata/; Federico Guerrini, *BMW Partners With IBM to Add Watson's Cognitive Computing Capabilities to Its Cars*, FORBES (Dec. 15, 2016, 9:44 AM), https://www.forbes.com/sites/federicoguerrini/2016/12/15/bmw-partners-with-ibm-to-add-watsons-cognitive-computing-capabilities-to-its-cars/#2e1257841a90. In June 2017, BMW and IBM announced a joint initiative to develop a cloud computing project linking different operating networks and data sources. The press release emphasizes the consent-based rights of the drivers to allow the collection and use of the data. https://www-03.ibm.com/press/us/en/pressrelease/52595.wss#release.

[190] Minister Alexander Dobrindt's approach to define the collected data as property of the car owner opens new discussions how the regulation of data ownership has to

Recall that unborn animals and growing crops are not yet classified as goods under the Uniform Commercial Code. Future data streams are similar; they do not yet exist, though their attributes, sources, and structures are predictably identifiable as byproducts of the design of the related technologies. For these future data streams, legal solutions similar to those for future goods can be deployed. A sale of future data can be structured, with the related agreements defining when control of the future data will commence and, if so negotiated, will be transferred, with details emphasizing the systems, processes, and records on which the parties shall rely.

In many respects, companies that see their operating data acquired by cloud-based service providers are situated no differently with respect to their data than data subjects are with respect to their personal information. We believe the preceding balances work just as effectively for both industrial data gathered by third parties from the operations of a company and PII gathered with respect to individual data subjects.

E. Allocating the Risks of Fictional Data

Recall that Part I of this paper introduced the terms "factual data" and "fictional data." In doing so, our focus was not on copyright protection for fictional works, including those in digital form. For those works, copyright law generally provides sufficient enforcement. Instead, we were contemplating how to address situations in which industrial data fails to pass relevant tests for assuring its authenticity as factual information.[192] As noted earlier, the U.S. Supreme Court concluded copyright law does not protect mere listings of "factual information."[193] But the analysis in that case, focused on telephone directory listings, did not require the Court to provide a measure of when data intended as factual is, in truth, fictional.

---

take into consideration how this approach fits to leased cars or the increasing number of shared cars.

[191] [The right of disposal shall be allocated to the data supplier. In principle this means: Data and the attributed rights belong to persons - in the case of vehicle data, to the registered keeper respectively owner of the car.] *See* BUNDESMINISTERIUM FÜR VERKEHR UND DIGITALE INFRASTRUKTUR, *supra* note 20.

[192] The issue occurs at any point in the information lifecycle of data. Of course, many security techniques exist to help verify the continued authenticity of information and protect the data from malicious conduct that seeks to manipulate the information itself. But the consequences of how to allocate responsibility for either the failure of security controls to be applied, or the ability to protect data across the larger commercial ecosystems in which data now circulates, remain significant commercial issues.

[193] *See* Feist, *supra* note 102.

A traditional warranty made in corporate acquisitions will require the seller to verify the integrity and authenticity of the information on which the transaction is based; similar warranties for data, structured into purchase agreements, licenses, and other commercial arrangements can be easily contemplated. But, where is the line of demarcation among the parties for how and where to transfer their responsibilities?

The *control* concept can be useful to define that line of demarcation. When control is transferred, so too can the responsibility for assuring the factual integrity of the subject data be transferred. Stated differently, the original owner, on asserting control, assumes the responsibility for sustaining the integrity of the data, and retains that responsibility until control is transferred.[194] Thus, the chain of title and control allow the chain of responsibility for data integrity to follow along in parallel.

While a full expression of how copyright laws should be reformed to support the Digital Age is beyond the scope of the paper, we suggest that copyright law could be conformed to protect fictional data as fully as possible, and enable property rights in industrial data and personal information (all of which is also factual data, including analytical output derived therefrom) to be explicit and governed by appropriate, unique controls such as proposed here.

F. Enabling Technologies

This proposal has been developed taking account of known, emerging technologies, notably blockchain distributed ledgers and zero-knowledge proofs, as well as existing cryptographic tools for securing the integrity of data.[195] We fully believe the proposal can be sustained with

---

[194] An astute lawyer might argue the original owner can only assure the integrity of the data collected by the related sensors, but disclaim responsibility for the accuracy of the sensors themselves. That secondary responsibility for the accuracy of the sensors becomes part of the negotiation for the purchase or use of the sensors.

[195] We note that Estonia, briefly surveyed in Part II, is proceeding forward with blockchain at the governmental level. *See, e.g.*, *Blockchain Technology in Estonia: What Happens at Governmental Level*, GLOBAL BANKING AND FIN. REV. (Mar. 8, 2017), https://www.globalbankingandfinance.com/blockchain-technology-in-estonia-what-happens-at-governmental-level/. Zero knowledge proofs ("ZK proofs") enable one party to mathematically prove the truth of an assertion about an asset to a second party (such as a seller describing a data asset to a buyer) without exposing the asset to the second party. Imagine buying a new automobile and being able to mathematically be convinced every statement about the attributes of the automobile are factually accurate. ZK proofs enable that outcome. ZK proofs are being actively explored in today's innovative maelstrom for data assets, including those secured on blockchain-based ledgers. *See, e.g.*, Nelson Petracek, *What Zero-*

these technologies, as well as improved as next generations of quantum-based cryptography are introduced (In-depth discussion of these technologies is beyond the scope of this paper).

Blockchain is, however, already being considered in the automotive industry. Online reports of initiatives by Toyota highlight that the technology may allow for pooling and sharing data among owners, fleet managers, manufacturers, insurance companies, and other stakeholders.[196] But, in those types of circumstances, the fundamental questions of ownership (and the related rights to control access, use, and further distribution or reuse) have not yet been resolved.

We believe the answers, when structured around identification, classification, and exercise of control, become entirely feasible to contemplate and structure into the existing web of commercial agreements among the varied stakeholders. Indeed, among the manufacturers and suppliers of components equipped with sensors, and software applications that create, process, store, or communicate data from a vehicle, the ownership and use of related industrial data will quickly become a commercially vital variable in their relationships.

CONCLUSION AND NEXT STEPS

Cognizant of international policy and industrial calls for explicit legal rights to own data, our research examined more closely the classifications of data on which those calls were focused. A classification scheme was developed and applied through new definitions that allow various distinctions to be made in evaluating how to build a construct of property rights for data.

The automotive industry was selected as a focal point of our analysis and, indeed, significant momentum was identified in that industry, in both Europe and Asia, to develop property rights principles, including in commercial agreements. Currently enacted laws and academic scholarship were surveyed to determine if two principles on which the proposed new construct is based have, in any degree, been recognized: namely the physical nature of data and the manner of attaching ownership to all

---

Knowledge Proofs Will Do for Blockchain (Dec. 16, 2017, 2:41 PM), https://venturebeat.com/2017/12/16/what-zero-knowledge-proofs-will-do-for-blockchain/.

[196] Philip E. Ross, *Toyota Joins Coalition to Bring Blockchain Networks to Smart Cars*, IEEE SPECTRUM (May 24, 2017, 2:02 PM), http://spectrum.ieee.org/cars-that-think/computing/networks/toyota-joins-coalition-to-bring-blockchain-networks-to-smart-cars; *see also Toyota Explores Blockchain Tech in Autonomous Cars*, AUTO. FLEET (May 22, 2017), http://www.automotive-fleet.com/channel/safety-accident-management/news/story/2017/05/toyota-explores-blockchain-tech-potential.aspx.

classifications of data through automated systems exercising control. Based on our research, we concluded those principles have not been recognized for data as a separate property classification. However, we also noted that economic models are advancing to monetize data as property that would benefit from greater clarity of ownership.

On the basis of the preceding, a construct is proposed to recognize ownership of data at the moment of creation and to enable ownership to attach to data through automated systems exercising control. Once ownership is attached through digital systems, the rights, privileges, controls, and constraints by which the subject data can be used may be expressed and enforced through electronic contracting mechanisms that are already in place across vast sections of the global marketplace. The suitability of that construct was considered, taking into account existing privacy laws and intellectual property protection laws, and we concluded that those laws can be reconciled with the notions of data ownership.

Since the 1980s, legal reforms to harness the potential of digital technologies have occurred with astonishing speed, particularly in comparison to the evolution across humankind of certain other established principles and governance concepts! Our collective experience during that time period confirms that legal solutions work best which deliver predictable, scalable, and extensible mechanisms for enabling new kinds of digital transactions. This article's proposal is designed to achieve those outcomes by leveraging and adapting appropriate legal structures that have already been negotiated and adopted by consensus, both in U.S. legal systems and, more recently, at the United Nations.

In other words, the consensus-based orientation of good rulemaking for electronic commercial practices has already produced useful work product that can, in turn, support the next steps needed to build additional rules and market mechanisms that will scale across nation-state, regional, and industry-specific solutions. The German and Japanese industry-specific materials referenced in this paper indicate the collaborations and potential to achieve even more are already underway. The Estonian digital government advances illustrate the applicability and potential at the nation-state level.

The next steps are not insubstantial in number or degree. Greater precision will be needed, and existing information governance and information security technologies and innovations must be considered more closely to assure that their adaptability to enable the proposal can be accomplished. But our hope is that the proposal made here will stimulate a more focused discussion on how ownership can be created, attached, and exercised to most fully advance the potential of our Digital Age.

Jeffrey Ritter
Testimony, US Senate Committee on
Banking, Housing, and Urban Affairs
October 24, 2019

Annex C

A hard copy of Achieving Digital Trust: The New Rules for Business at the Speed of Light has been delivered to the Committee staff as part of this written testimony.

PREPARED STATEMENT OF CHAD A. MARLOW

SENIOR ADVOCACY AND POLICY COUNSEL
AMERICAN CIVIL LIBERTIES UNION

OCTOBER 24, 2019

Chairman Crapo, Ranking Member Brown, and Members of the Committee on Banking, Housing, and Urban Affairs, on behalf of the American Civil Liberties Union (ACLU),[1] I want to thank you for the privilege of testifying before your Committee today.

The ACLU is strongly concerned about the data-as-property model and how it is being presented to the American public and its lawmakers. While the data-as-property model may have merit as a tool for redistributing the money that is currently being made off the sale of personal information, any claim that it advances privacy is false. To the extent Congress is seeking to provide greater private protections for Americans' personal information, what we need is an affirmative consent-based model that provides all individuals the ability to opt-in (or not) to the sharing of their personal data. Whether consenting to such use results in monetary gain is a separate matter, and does not in and of itself advance privacy. We should not countenance misleading assertions that the data-as-property model is itself pro-privacy.[2]

A central tenet of the data-as-property model is that the Government should establish—through regulating and policing a universal marketplace of personal data—that individuals are "owners" of their personal information and, consequently, have a property-based right to sell or refuse the sale of their data to third parties. However, if the objective is privacy protection, policymakers have identified other approaches that more directly facilitate advancements in the cause of personal information privacy and do not carry the adverse privacy risks associated with the data-as-property approach. For example, two State laws passed last year[3]—the "California Consumer Privacy Act,"[4] which allows consumers to opt-out of their personal information being sold, and Maine's "Act To Protect the Privacy of Online Customer Information,"[5] which takes the superior approach of not allowing a person's information to be sold without first securing their "opt in" permission—made important advances in protecting individual privacy, without treating data as property or focusing on its monetary value. Rather, they advanced privacy by empowering individuals to exercise control over their personal information. Indeed, at a time when our existing laws at the Federal level and in most States are wholly insufficient to ensure that individuals have control over protecting their personal information, the data-as-property model simply distracts us from pursuing meaningful privacy legislation.

Four aspects of the data-as-property model—which essentially mandates the creation of a Government-regulated and policed marketplace for personal information—would be especially harmful to privacy and free speech:

Creating Conflict at the Time Individuals Might Otherwise Choose To Protect Their Personal Information

To understand why the data-as-property model is concerning, one should start by looking to how it would be effectuated. Namely, at the time a person's information is collected—which is when pro-privacy laws typically mandate the disclosure of one's data privacy rights—a Government mandate would require the simultaneous advertising of the individual's ability to surrender their privacy by selling their personal information. To make the decision to sell one's data seamless, where this

---

[1] For nearly 100 years, the ACLU has been our Nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. With more than eight million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 States, Puerto Rico and Washington, DC, to preserve American democracy and an open Government.

[2] Chad Marlow, *Beware the Tech Industry's Latest Privacy Trojan Horse,* ACLU (Mar. 18, 2019), *https://www.aclu.org/blog/privacy-technology/medical-and-genetic-privacy/beware-tech-industrys-latest-privacy-trojan.*

[3] Francoise Gilbert, *Maine Follows California Lead: Prohibits ISP Use, Sale, Disclosure of Online Consumer Information Without Prior Affirmative Consent,* The National Law Review (June 10, 2019), *https://www.natlawreview.com/article/maine-follows-california-lead-prohibits-isp-use-sale-disclosure-online-consumer.*

[4] SB–1121, 2017–2018 Leg., (Cal. 2018) also available at *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.*

[5] S.P. 275, 2019 Leg., 129th Sess. (Me. 2019) also available at *http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=1&snum=129.*

model has been pushed by data sales facilitators on the State level, the bills further require data sales authorization forms be concurrently provided.

Imagine, as was the focus of a data-as-property bill in Oregon earlier this year, how uncomfortable that exchange might be where, in the course of ongoing medical treatment, a doctor requests a patient provide consent so they can sell the patient's personal information. Now further imagine what pressure might be applied where the doctor has been incentivized to secure consent by being offered a cut of the sale revenue for the data.

Instead of giving consumers meaningful control over their personal information, many of the private sector entrepreneurs who are advocating for the data-as-property model want to use the power of the Government to mandate that the marketplace for selling data—one they will very profitably help to facilitate—is advertised to all persons at the time their information is collected. We have seen this as a central feature of the data-as-property bills being introduced in States, like the previously referenced bill in Oregon,[6] where as soon as the bill was understood to be a privacy Trojan Horse, it was soundly rejected. In fact, no data-as-property bill has been adopted in any of the States in which they have been pursued or introduced, which includes Oregon, Maryland, Hawaii, California, Washington, Montana, Arizona, Georgia, New Jersey, Massachusetts, and Pennsylvania.

If anything, when it comes to privacy, what the data-as-property model actually does is create a hedge against the growing likelihood that Congress and the States will pass tougher privacy laws. Specifically, it would ensure that, should stronger privacy protections be implemented, the data sales marketplace—which relies upon convincing people to relinquish their privacy—will be advertised right alongside any required notifications about individuals' new privacy rights. As Congress explores how to better protect Americans' privacy, it should strongly resist supporting the data-as-property model, which would undermine those efforts to directly protect privacy.

Widening of Digital Divide and Disproportionate Harm to the Most Vulnerable Individuals

The high value Americans place on their privacy is universal[7] and nonpartisan.[8] It is wisely enshrined in our Bill of Rights.[9] As a result, adopting a model where persons with less wealth are likely to end up with less privacy should give lawmakers pause.

Americans who are economically secure will find it easy to reject offers to surrender their private information in order to make a few extra dollars. But that might not be the case for an elderly person who has a hard time affording their prescriptions and rent. It may be too tempting a sales pitch for a family that is struggling to put food on their table. For persons who live in rural areas, where the cost of online access may already be steep, a chance to offset those costs while online may feel impossible to turn down. And so they will agree, when pressed, to sell their private information for an unquantified amount of money.

As a consequence, a Government-endorsed data-as-property model would only serve to further expand this country's existing digital divide,[10] where persons already enduring socioeconomic or regional economic disadvantages—including disproportionately, persons of color—frequently have little or no choice but to rely on cheaper, non-encrypted cell phones, free email, and other more affordable but less secure tech products. The digital divide is a privacy divide, and the data-as-property model would only serve to worsen it.

Requirement of a Universal Unique Tracking Identifier for All Persons

One of the most pernicious practical requirements of any data-as-property model would be the need to create some form of universal unique tracking identifier for all personal information. To track who owns personal data, who has sold it, who

---

[6] S.B. 703, 2019 Leg., 80th Sess. (Or. 2019) *https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/SB703/Introduced.*

[7] NATIONAL SCIENCE BOARD, AMERICANS' ATTITUDES TOWARD INFORMATION PRIVACY IN THE WORLD OF BIG DATA at 1, also available at *https://nsf.gov/statistics/2018/nsb20181/assets/404/americans-attitudes-toward-information-privacy-in-the-world-of-big-data.pdf.*

[8] Carl M. Cannon, *Digital Privacy, a Non-Partisan Issue,* Real Clear Politics (July 23, 2013) *https://www.realclearpolitics.com/articles/2013/07/23/digital__privacy__a__non-partisan__issue__119332.html.*

[9] U.S. Const. amend. IV.

[10] Gry Hasselbach and Pernille Tranberg, *Privacy is creating a new digital divide between the rich and poor,* The Daily Dot (Oct. 23, 2016), *https://www.dailydot.com/layer8/online-privacy-data-ethics/.*

must pay, and who gets paid, each piece of data must be tagged with some form of a universal identifier.

There likely would be no opt-out from a universal unique tracking identifier for anyone, even for those who consistently refuse to sell their personal information. Why? Because legal compliance is likely to not only require companies to identify what data they are permitted to sell and resell, but also to identify unlawfully distributed data as to which sales permission has been denied.

The need for a universal unique tracking identifier gets particularly apparent, as well as difficult to implement as the lines blur on who owns what data. What happens when data is sold that has information about multiple parties, like DNA or a group photo? Does everyone have to agree and get paid? What happens when some parties whose personal information is contained is data elected to sell it and others refuse? Who prevails?

In the end, whether people choose to sell their personal information or not, the effectuation of the data-as-property model, including the universal unique tracking identifier it may require be attached to all personal data, raises significant privacy concerns.

Harm to Free Speech on the Internet

The need to track all communicated personal information, in order to effectuate and enforce the data-as-property model, will have an adverse impact on free speech. For example, every time a person shares content on the internet, sends an email or text message over a public network or using a free application, or posts a picture of themselves or their family or friends on social media, personal information about them will be transmitted, either within the communication itself or in its accompanying metadata. As a result, under the data-as-property model, it will need to be tracked and associated with the person who communicated it using a universal unique tracking identifier. Once the public becomes aware of this fact—and if the ACLU doesn't warn them, one of dozens of other privacy organizations certainly will—the public will know it has lost the ability to communicate anonymously.

This would have an adverse effect on the free exchange of ideas, including on the ability to communicate private thoughts, or messages intended for a limited audience, or ideas that are either unpopular or represent opinions one is exploring but does not necessarily endorse. Privacy and free speech frequently go hand in hand, and that is certainly the case with the harms presented to them by the data-as-property model.

A Better Way: Adopt Meaningful Privacy Legislation

If Congress wants to pass a law that creates meaningful privacy protections for Americans—if Congress wants to pass a law so that every time Americans use the internet, or social media, or complete a commercial transaction, they do not have their personal information gathered and offered up for sale to third parties—it does not need to treat data as property to do so. In fact, passing legislation that treats data as property carries specific harms that would undermine that goal.

The Government should not be promoting privacy as a resource to be bought and sold. A growing number of State constitutions[11] now recognize that privacy is a fundamental right, including the constitutions of the home States of this Committee's Members from Arizona, Hawaii, Louisiana, Montana, and South Carolina, along with many others.

The proper response to the pervasive loss of individual privacy is to pass stronger privacy laws,[12] not just to throw up our hands and conclude the only issue left to tackle is who gets the money when people's data is sold. Yes, privacy protections for personal information are weak in this country, but Congress and the States have the ability to strengthen them. And they should. Limiting data collection, retention, and further transfers without a person's clear, distinct, and informed permission is a strong place to start.

Additionally, companies should be prohibited from denying a good or service to someone who chooses to exercise their privacy rights, and consumers should have a private right of action to seek compensation when their privacy rights are

---

[11] Privacy Protections in State Constitutions, National Conference of State Legislatures (Nov. 7, 2018) *http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.*

[12] *Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework Before the S. Comm. On Commerce, Science, and Transportation,* 116th Cong. 3 (2019) (statement of Neema Singh Guliani, Senior Legislative Counsel, ACLU) also available at *https://www.commerce.senate.gov/services/files/79ABFD7A-8BEB-45B5-806A-60A3467255DD.*

violated. Most relevant to today's discussion, we should not be looking to a data-as-property model, which monetarily incentivizes people to give up their privacy, to enhance privacy protections.

Again, if those who support the data-as-property model want to talk about it as a potential way to create a more robust and equitable marketplace for the sale of personal data, by all means they should make that argument, but they need to stop advancing the false narrative that the data-as-property model is pro-privacy.

Congress has the ability to adopt laws that truly empower Americans to better protect their personal information without undermining privacy in the process, and I have confidence that you will.

Thank you again for the opportunity to testify today. I look forward to answering your questions.

PREPARED STATEMENT OF WILL RINEHART

DIRECTOR OF TECHNOLOGY AND INNOVATION POLICY
AMERICAN ACTION FORUM*

OCTOBER 24, 2019

Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for the opportunity to testify today regarding data property rights. Like many privacy experts, I'm skeptical that data property rights are the best policy mechanism for ensuring privacy is secured in the digital age. I hope to make three main points today:

- A property right to personal data isn't needed to establish consumer privacy rights, nor would it be economically efficient to establish this kind of property right;
- Valuing personal data is difficult because raw or personal data per se is not what is in demand, but rather the insights that can be gleaned from that data-insights that often depend on the data's environment; and
- Regardless of the particular policy mechanism, privacy laws will create unavoidable costs from compliance, which will impact investment opportunities in countless industries.

The Purposes and Limitations of Propertization

With Congress again considering Federal privacy legislation, the idea of personal data property rights is being explored as one policy mechanism for securing privacy.[1] The very phrase "personal data" conjures up the notion that individuals own that data and firms are merely taking it. Data propertization, which is the creation of property rights in law, has been seen as an attractive alternative since the 1970s, for two reasons.[2] First, it would grant individuals the ability to sell their personal data, thus allowing them to recapture some of its value. Second, propertization would force companies to internalize the costs of disclosure, thereby aligning firm and user expectations about data collection and use since users would be able to bargain over the terms of the deal.[3]

There are reasons to be skeptical that assigning property rights in data will have unalloyed benefits. For one, assigning property rights to data is a contortion of the normal reasoning that underpins intellectual property (IP) rights such as copyright and patents. Information, which is embodied in copyrights and patents as well as user data, can be easily reproduced (*i.e.,* is nonrivalrous), and it is difficult to prevent nonpaying consumers from accessing it (non-excludable). Property rights, incentivize information creation, since those rights give the holder the ability legally to exclude others, thus making the information rivalrous. Yet, the problem faced in privacy is of the opposite kind—the purpose is to limit information disclosure.

Second, it is unclear if the assignment of data property rights will align incentives between users and firms. While it is the case that information disclosure can either be beneficial or detrimental, users cannot know beforehand if the use of their data

---

*The views expressed here are my own and do not represent the position of the American Action Forum.

[1] Michael Gorthaus, "Andrew Yang proposes that your digital data be considered personal property," available at: *https://www.fastcompany.com/90411540/andrew-yang-proposes-that-your-digital-data-be-considered-personal-property.*

[2] Alan Westin, *Information Technology in a Democracy.*

[3] Pamela Samuelson, "Privacy As Intellectual Property," available at: *https://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf.*

will necessarily lead to better products.[4] Data propertization would only exacerbate this problem, forcing users to search for the best value for their data. In other words, data property rights would make users data entrepreneurs. Searching for innovative opportunities is costly, and thus one could imagine that users will likely hire an intermediary to do this task—which is the job of platforms and other data providers presently.

As is detailed in an appendix to this paper, the Hart-Grossman-Moore model of property helps to flesh out the idea. This model can help to determine where it is most efficient to allocate property rights. When one party's investment in the data does not boost the total value that much, then it is better for the other party to have control of the assets. In the parlance of economics, the party with higher marginal returns from investment should be given the rights of control, which is why platforms, and not users, spend so much time and effort to understand what is happening on the platform. Assigning data property rights to users will likely be inefficient because it will change the investment decision veto point.

Third, and most important for this Committee, real world implementation will prove tricky because of the interconnected nature of information. The vast majority of data generated in the last decade comes from user interactions with online platforms. If Google didn't exist, there would be no search data. If Facebook didn't exist, there wouldn't be social graph data. To understand the challenge of implementing data property rights, it is helpful to recognize how three classes of data interact in online platforms.[5] *Volunteered data* is data that is both innate to an individual's profile, such as age and gender, and information they share, such as pictures, videos, news articles, and commentary. *Observed data* comes as a result of user interactions with the volunteered data; it is this class of data that platforms tend to collect in data centers. Last, *inferred data* is the information that comes from analysis of the first two classes, which explains how groups of individuals are interacting with different sets of digital objects. At the very least, then, data is a co-created asset, with the users providing volunteered data and the platform assembling observed data to create inferred data. Creating data property rights will likely necessitate that only one party has rights, which has been a sticking point for previous efforts.

As the German government discovered when trying to implement data property for connected cars, determining the owner isn't simple. Does the car company own the property right, or might it be the driver, or even the rider?[6] Privacy scholar Robert Gellman demonstrated this problem would also beleaguer health care. For example, information about a child's health could simultaneously belong to the patient, the patient's family, the school, the pharmacy, the supermarket, the pediatrician, the drug manufacturer, social media platforms, advertising companies, or internet service providers.[7] Questions of fuzzy ownership continually plague IP and would similarly afflict data property.

Further, and even more practically, a property right in data isn't needed to establish consumer privacy rights. For evidence of this fact, one only needs only to consult the current laws in the United States. The Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), and the California Consumer Privacy Act (CCPA), just to name a few, all protect privacy without creating property rights. As Stanford Law Professor Lothar Determann has said quite bluntly, "no one owns data" because data are already "subject to a complex landscape of access rights and restrictions."[8] Privacy regulation already defines certain kinds of entitlements to control and contract upon data. Adding a superordinate property right on top of these existing restrictions would make the entire enterprise all that more complicated and undermine current efforts to grant consumers control. If data property rights were implemented, for example, would an individual be able to limit critical information from being shared with credit rating agencies?

Determann isn't the only scholar of privacy who opposes propertization efforts. Technologist Larry Downes has been critical of the idea and instead prefers the current licensing model since it "recognizes that most information with economic value

---

[4] Alessandro Acquisti, Curtis R. Taylor & Liad Wagman, "The Economics of Privacy," available at: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411.*

[5] World Economic Forum, "Personal Data: The Emergence of a New Asset Class," available at: *http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.*

[6] Lothar Determann, "No One Owns Data," available at: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3123957.*

[7] Robert Gellman, "Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges," available at: *https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf.*

[8] See footnote 6.

is the collaborative creation of multiple sources, including individuals and service providers."[9] Law Professor Julie Cohen has argued against privacy as property as well since it doesn't uphold the values of autonomy and participation that are so central to privacy.[10] European law professor Bart Schermer agreed with Cohen when the issue was raised in 2015 as an alternative to the European Union's (EU) General Data Protection Regulation (GDPR), saying that "Reducing the discussion about privacy and personal data to a discussion about ownership oversimplifies the discussion about privacy in the information society and may lead to sub-optimal results when it comes to regulating the use of personal data."[11] But Dr. Mark MacCarthy of Georgetown University said it best, laying out the world of data property rights as "a privacy nightmare rather than a privacy paradise."[12] As much as there is disagreement in privacy advocacy and scholarship, there is consistent agreement that propertizing data has serious limits.

Finally, pricing data, which is one stated goal of data property rights, will have deleterious effects on privacy expectations. As Jason Aaron Gabisch and George R. Milne reported in the Journal of Consumer Marketing, "The findings show that receiving compensation, especially when it is a monetary reward, reduces consumer expectations for privacy protection."[13]

Valuing Data

Four methods can be employed to value intangibles such as data: income-based methods, market rates, cost methods, and shadow prices.

Most popular data valuations are accomplished through income derivations, often by simply dividing the total market capitalization or revenue of a firm by the total number of users. For those in finance, this method seems most logical since it is akin to an estimate of future cash-flows. In a *Wired* article, for example, Antonio Garcia Martinez placed an upper bound of $112 on the value of data for users in the United States, citing Facebook's 2018 annual report.[14] Similarly, when Microsoft bought LinkedIn, reports suggested that it was buying monthly active users at a rate of $260 per user.[15] Stanford Law Professor A. Douglas Melamed argued before the Senate Judiciary that the upper-bound value on data should at least be cognizant of the acquisition cost for advertisements—putting the total value per user at around $16.[16]

Still, these income-based valuations aren't exact estimates because they are not capturing a user's ability to marginally earn revenue, which is where the price would be set. As noted before, inferential data is the key for platform operators, as it drives advertising decisions and helps determine what content is presented to users. Thus, the ultimate value of a user's data would combine the value of that user's data to increase all their friend's demand for content and the value of that user's data to contribute to increases in advertising demand. Calculating marginal income valuations in this manner are difficult, but Shapley values have been shown as a viable method theoretically.[17, 18] Still, it remains unclear if firms would be able to implement this method on their platform.[19] Needless to say, income-based valuations are difficult.

---

[9] Larry Downes, "A Rational Response to the Privacy 'Crisis,'" available at: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200208.*

[10] Julie E. Cohen, "Examined Lives: Informational Privacy and the Subject as Object," available at: *https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub.*

[11] Bart Schermer, "Privacy and property: do you really own your personal data?" available at: *https://leidenlawblog.nl/articles/privacy-and-property-do-you-really own-your-personal-data.*

[12] Mark MacCarthy, "Privacy Is Not A Property Right In Personal Information," available at: *https://www.forbes.com/sites/washingtonbytes/2018/11/02/privacy-is-not-a-property-right-in-personal-information/.*

[13] Jason Aaron Gabisch & George R. Milne, "The impact of compensation on information ownership and privacy control," available at: *https://www.emerald.com/insight/content/doi/10.1108/JCM-10-2013-0737/full/html.*

[14] Antonio Garcia-Martinez, "No, Data Is Not the New Oil," available at: *https://www.wired.com/story/no-data-is-not-the-new-oil/.*

[15] James E. Short & Steve Todd, "What's Your Data Worth?" available at: *https://sloanreview.mit.edu/article/whats-your-data-worth/.*

[16] A. Douglas Melamed, "Prepared Statement," available at: *https://www.judiciary.senate.gov/download/melamed-testimony.*

[17] Amirata Ghorbani & James Zou, "Data Shapley: Equitable Valuation of Data for Machine Learning," available at: *https://arxiv.org/abs/1904.02868.*

[18] Eric Bax, "Computing a Data Dividend," available at: *https://arxiv.org/pdf/1905.01805.pdf.*

[19] While Bax has shown that Shapley values can be implemented in polynomial time, it is unclear if Shapley values that exhibit demand interdependencies could be implemented in polynomial time as well.

Second, market prices are another method of valuing data, and they tend to place the lowest premium on data. For example:

- Vice recently reported that Departments of Motor Vehicles across the United States have been selling individual records for as little as one cent each;[20]
- *Wired* editor Gregory Barber sold his location data, Apple Health data, and Facebook data, and all he got was a paltry $0.003 for everything together;[21]
- After a breach at Facebook, Facebook logins were selling on the dark web for $2.60 per user;[22]
- Advertisers typically pay $0.005 for complete profile for an individual;[23]
- General information about a person, such as their age, gender, and location is worth a mere $0.0005 per person, or $0.50 per 1,000 people;[24]
- Auto buyers are worth about $0.0021 per person, or $2.11 for every 1,000 people;[25] and
- For $0.26 per person, buyers can access lists of people with specific health conditions or taking certain prescriptions.[26]

In reviewing these estimates, *The Financial Times* noted that "the sum total for most individuals often is less than a dollar." It is worth noting that sub $1 payments have been unprofitable for firms to process due to the fixed technical costs for developing the backend architecture and hardware, storage costs for transaction integrity and legal purposes, computational costs for processing payments, communication costs for information transfer, and administrative costs.[27]

As with any market, it is important to pay attention to the difference between the clearing price and the asking price. The bankruptcy proceedings for Caesars Entertainment, a subsidiary of the larger casino company, offers a unique example of this problem. As the assets were being priced in the selloff, the Total Rewards customer loyalty program got valued at nearly $1 billion, making it "the most valuable asset in the bitter bankruptcy feud at Caesars Entertainment Corp."[28] But the ombudsman's report understood that it would be a tough sell because of the difficulties in incorporating it into another company's loyalty program. Although it was Caesar's asset with the highest valuation, its real value to an outside party was an open question.

The Total Rewards example underscores an important characteristic of data: It is often valued within a relationship but is difficult to value outside of it. Within economics, there is a term for this phenomenon, as economist Benjamin Klein explained: "Specific assets are assets that have a significantly higher value within a particular transacting relationship than outside the relationship."[29] Asset specificity helps to explain why there isn't an auction market for personal data. It isn't the raw data that is in demand, but the insights that can be gleaned from that data.

Third, data might be valued using cost-based methods, but this method also has shortcomings. Proxying the value of data by summing the salaries of data analysts and the costs of data centers will likely underestimate the value of data. Data is an intermediate product for other business processes. In practice, cost-based methods would probably look like Shapley values anyway.

Last, data can be valued through shadow prices.[30] For those items that are rarely exchanged in a market, prices are often difficult to calculate, so other methods are used to appraise what is known as the shadow price. For example, a lake's value might be determined by the total amount of time in lost wages and money spent

---

[20] Joseph Cox, "DMVs Are Selling Your Data to Private Investigators," available at: *https://www.vice.com/en_us/article/43kxzq/dmvs-selling-data-private-investigators-making-millions-of-dollars?utm_campaign=sharebutton.*

[21] Gregory Barber, "I Sold My Data For Crypto, Here's How Much I Made," available at: *https://www.wired.com/story/i-sold-my-data-for-crypto/.*

[22] Dan Hall, "Hackers selling Facebook logins on the dark web for $2," available at: *https://nypost.com/2018/10/01/hackers-are-selling-facebook-logins-on-the-dark-web-for-2/.*

[23] Frank Pasquale, "The Dark Market for Personal Data," available at: *https://www.nytimes.com/2014/10/17/opinion/the-dark-market-for-personal-data.html.*

[24] Financial Times, "Financial worth of data comes in at under a penny a piece," available at: *https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de.*

[25] *Ibid.*

[26] *Ibid.*

[27] Ioannis Papaefstathiou, "Evaluation of Micropayment Transaction Costs," available at: *http://web.csulb.edu/journals/jecr/issues/20042/Paper3.pdf.*

[28] Kate O'Keeffe, "Real Prize in Caesars Fight: Data on Players," available at: *https://www.wsj.com/articles/in-caesars-fight-data-on-players-is-real-prize-1426800166.*

[29] Benjamin Klein, "Asset specificity and holdups," available at: *http://masonlec.org/site/files/2012/05/WrightBaye_klein-b-asset-specificity-and-holdups.pdf.*

[30] Anthony E. Boardman, David H. Greenberg, Aidan R. Vining, & David L. Weimer, *Cost Benefits Analysis Concepts and Practice.*

by recreational users to get there. Similarly, the value of social media data might be calculated by tallying all of the forgone wages in using the site. A conservative estimate from 2016 suggests that users spend about fifty minutes a day month on Facebook properties.[31] Since the current average wage is about $28, this calculation indicates that people roughly value the site by about $8,516 over the entire year.[32] A study using data from 2016 using similar methods found that American adults consumed 437 billion hours of content on ad-supported media, worth at least $7.1 trillion in terms of foregone wages.[33]

Shadow prices can also be calculated through surveys, which is where this method gets particularly controversial. Depending on how the question is worded, users' willingness to pay for privacy can be wildly variable. Trade association NetChoice worked with Zogby Analytics to find that only 16 percent of people are willing to pay any price for online platform service.[34] Strahilevitz and Kugler found that 65 percent of email users, even though they knew their email service scans emails to serve ads, wouldn't pay for an alternative.[35] As one seminal study noted, "most subjects happily accepted to sell their personal information even for just 25 cents."[36] Using differentiated smartphone apps, economists were able to estimate that consumers were willing to pay a one-time fee of $2.28 to conceal their browser history, $4.05 to conceal their list of contacts, $1.19 to conceal their location, $1.75 to conceal their phone's identification number, and $3.58 to conceal the contents of their text messages. The average consumer was also willing to pay $2.12 to eliminate advertising.[37]

In all, there is no one single way to estimate the value of data, and none of them is particularly easy to implement.

The Impact of New Privacy Laws

Regardless of the path that is taken, new privacy laws will have both direct and indirect impacts on the economy, best seen in the wake of the GDPR and estimates from the CCPA. First, privacy regulation will force firms to retool data processes, known as refactoring, to comply with new demands. This refactoring is generally a one-time fixed cost that raises the cost of all information-using entities. Second, the regime will add risk compliance costs, causing companies to staff up to ensure compliance. Finally, privacy laws change the investment dynamics of the affected industries, as the market shifts to account for the newly expected returns.

Currently, the retooling costs and risk compliance costs are going hand in hand, so it is difficult to determine the costs of each. Still, they are substantial. A McDermott-Ponemon survey on GDPR preparedness found that almost two-thirds of all companies say the regulation will "significantly change" their informational workflows. According to this survey, the average budget for getting to compliance tops $13 million. The International Association of Privacy Professionals estimated that GDPR will cost Fortune 500 companies around $7.8 billion, and these won't be one-time costs since "Global 500 companies will be hiring on average five full-time privacy employees and filling five other roles with staff members handling compliance rules." A PwC survey on the rule change in Europe found that 88 percent of companies surveyed spent more than $1 million on GDPR preparations, and 40 percent more than $10 million.

Refactoring and compliance costs are adding up for CCPA as well. California's standardized regulatory impact assessment (SRIA) for CCPA calculated the total

---

[31] James B. Stewart, "Facebook Has 50 Minutes of Your Time Each Day. It Wants More." available at: *https://www.nytimes.com/2016/05/06/business/facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html.*

[32] Bureau of Labor Statistics, "Average hourly and weekly earnings of all employees on private nonfarm payrolls by industry sector, seasonally adjusted," available at: *https://www.bls.gov/news.release/empsit.t19.htm.*

[33] David S. Evans, "The Economics of Attention Markets," available at: *https://www.competitionpolicyinternational.com/the-economics-of-attention-markets/.*

[34] NetChoice, "American Consumers Reject Backlash Against Tech," available at: *https://netchoice.org/american-consumers-reject-backlash-against-tech/.*

[35] Lior Stahilevitz & Matthew B. Kugler, "Is Privacy Policy Language Irrelevant to Consumers?" available at: *https://papers.ssrn.com/sol3/papers.cfm?abstract__id=2838449.*

[36] Jens Grossklags & Alessandro Acquisti, "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information," available at: *https://www.econinfosec.org/archive/weis2007/papers/66.pdf.*

[37] Scott J. Savage & Donald M. Waldman, "The Value of Online Privacy," available at: *https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5735f456b654f9749a4afd62/1463153751356/The__value__of__online__privacy.pdf.*

costs at $55 billion, which is nearly 1.8 percent of the total gross State product.[38] The range of affected firms is massive. On the bottom end of the estimate, 15,643 businesses could feel an impact. On the top end, 570,066 companies will have to come into compliance with the law. Most alarming, the authors conclude that "economic impact of the regulations on these businesses located outside of California [that serve California consumers] is beyond the scope of the SRIA and therefore not estimated." If something akin to the California law were applied to the United States, the Information Technology and Innovation Foundation estimated the cost at $122 billion per year.[39]

Finally, privacy laws will surely change the investment and market dynamics in countless industries. When the EU adopted the e-Privacy Directive in 2002, Goldfarb and Tucker found that advertising became far less effective, which reverberated throughout the ecosystem as venture capital investment in online news, online advertising, and cloud computing dropped by between 58 to 75 percent. In Chile, for example, credit bureaus were forced to stop reporting defaults in 2012, which was found to reduce the costs for most of the poorer defaulters, but raised the costs for nondefaulters. Overall the law led to a 3.5 percent decrease in lending and reduced aggregate welfare. Early research on the GDPR has also found drops in investment. While much smaller than the United States, EU venture funding decreased by decreased 39 percent while the total number of deals saw a 17 percent drop.[40]

Conclusion

The dilemma for this Committee and others within Congress is hardly enviable. America's privacy pandect is complex, making difficult the task of creating new laws to enhance consumer privacy. While there is much disagreement in the privacy community, there is widespread agreement that data property rights are an unwieldy way of doing things. There should be no delusions, however, about the impacts. There will be serious costs involved with any new law. As Seth Godin once remarked, "The art of good decisionmaking is looking forward to and celebrating the tradeoffs, not pretending they don't exist." That is sage advice for any privacy legislation.

Technical Appendix

One way to understand this bargain is through the Grossman-Hart-Moore model, which considers a relationship between two risk-neutral parties, a buyer and a seller, or *B* and *S*. For this exercise, let's assume that the buyer of the data, *B,* is the platform, and the seller of the data, *S,* is the user, and again let's just work with the singular transaction. As such, the platform buys data, which is an intermediate good, from the users to create a final output. The value of the final good is *V(e),* which is contingent on *e,* a variable for the investment into the process by the platform. Similarly, the cost of the intermediate good is *C(i),* which is contingent on the investment, *i,* in the process conducted by the user.

There are two periods. In the first period, each party undertakes some kind of investment and in the second period, they decide to trade at a specific price, *p.* If they don't end up trading, they can turn to others and do so. A key assumption of this model is that the investments in the first time period are not contractible.

---

[38] Berkeley Economic Advising and Research, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," available at: *http://www.dof.ca.gov/Forecasting/Economics/Major__Regulations/Major__Regulations__Table/documents/CCPA__Regulations-SRIA-DOF.pdf.*

[39] Alan McQuinn & Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law," available at: *https://itif.org/sites/default/files/2019-cost-data-privacy-law.pdf.*

[40] Jian Jia, Ginger Jin & Liad Wagman, "The short-run effects of GDPR on technology venture investment," available at: *https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment.*

The social optimum would involve maximizing the total benefits minus the investment costs:

$$max_{e,i}\ \{V(e) - C(i) - e - i\}$$

Optimal investment thus occurs when

$$V'(e) = 1 \text{ and } -C'(i) = 1$$

But in the present set up, each party will only retain half of the gains from trade, such that

$$max_e \left\{\frac{V(e)}{2} - e\right\} \text{ and } max_i \left\{\frac{-C(i)}{2} - i\right\}$$

Because the parties will have to bargain over how to split the total surplus, each will get half of the benefits from their investment. See Aghion and Holden (2011) for further details on the Nash bargaining.[41] Thus, each party will underinvest relative to the first best.

If the parties instead have vertically integrated, the result is slightly different. If, say, B controls the total gains from the production processes, then B will invest at their first best level while S will underinvest. Similarly, if S were to own total gains, then S will invest at their first best, while B will underinvest.

This model yields some interesting insights. It is important to note that, like the rest of the literature in this space, the investment elasticities are key. Since S or users, have extremely inelastic investment decisions, that is, they don't change that much with the possibility of B appropriating them, it is the case that B should own the total gains.

This makes sense in the case of platforms. The investment that matters the most lies in the inference data of the platform. Users have indeed tried to sell their own "investment," but these transactions don't yield much. Moreover, the relative investments speak to why data ownership efforts are likely to fail. Since the marginal returns for any user S is much higher when a platform B controls both, as compared to when users simply "own their data," independent ownership is likely to lead to inefficient gains for all sides.

[41] Philippe Aghion & Richard Holden, "Incomplete Contracts and the Theory of the Firm: What Have We Learned over the Past 25 Years?" available at: *https://www.aeaweb.org/articles?id=10.1257/jep.25.2.181.*

PREPARED STATEMENT OF MICHELLE DENNEDY*

CHIEF EXECUTIVE OFFICER, DRUMWAVE, INC.

OCTOBER 24, 2019

Introduction

The world is certainly flat. Everyone said so. The government said so. The church said so. Your wise old aunt and the richest guy in town said so. Everyone.

Except, a few explorers, dreamers, scientists, artists, and plain-spoken folks who looked out at a sky that looked more like a bowl and noticed that the ground and sky always met for a brief kiss before the observer wandered ever closer and the meeting became elusive. And shadows, tides, and other indications seemed to suggest that there might be something more than dragons beyond the edge of the world. And so, as it turned out, the world was not, in fact flat. There was a seemingly endless set of new possibilities to discover.

Privacy is *certainly* dead. Everyone said so. Rich people with big boats who sold stuff to the CIA in the 1970s said so. Founders of important hardware companies said so. Someone who blogs said so. The government cannot make up its mind which person should say so or if the polling numbers look right, but it might say so. Someone tweeted. Even really old technologists who helped invent the whole thing said so. *Everyone*.

Except, a few explorers and inventors and philosophers and children and parents and even government regulators who looked out at a seemingly endless sea of data and could still see how a person can be distinguished from a pile of metadata. This is true for people who wish to decide for themselves the story they wish to tell about themselves and see a different horizon. The privacy engineer sees this horizon where privacy and security combine to create value as a similarly challenging and exciting time for exploration, innovation, and creation; not defeat.

The purpose of this book is to provide, for data and privacy practitioners (and their management and support personnel), a systematic engineering approach to develop privacy policies based on enterprise goals and appropriate government regulations. Privacy procedures, standards, guidelines, best practices, privacy rules, and privacy mechanisms can then be designed and implemented according to a system's engineering set of methodologies, models, and patterns that are well known and well regarded but are also presented in a creative way. A proposed quality assurance checklist methodology and possible value models are described. But why bother?

The debate about data privacy, ownership, and reputation poses an irresistible and largely intractable set of questions. Since the beginning of recorded history, people have sought connection, culture, and commerce resulting from sharing aspects about themselves with others. New means of communication, travel, business, and every other social combination continue to evolve to drive greater and greater opportunities for the solo self to be expressed and to express oneself in person and remotely. It is all terribly exciting. Yet, every individual desires a sense of individuality and space from his or her fellow man; a right to be left alone without undue interference and to lead his or her individual life.

*Statement is an excerpt from *The Privacy Engineer's Manifesto.* Michelle Dennedy, Jonathan Fox, & Thomas R. Finneran (2014). Apress.

Governments have played a stark role in the development of data privacy. Laws are created to protect, but there are also abuses and challenges to individual rights and freedoms in the context of multiple governments in a world where people have become free to travel with relative ease and comfort—sans peanuts—around the globe and back again. National and international security norms have been challenged in both heroic and embarrassing fits and starts. The role of total information vs. insight and actionable information is debated again and again. "Insiders" and fame seekers have exposed massive data collection programs.

In the information technology sector, data privacy remains a matter for heated debate. At times the debate seems as if technologists somehow wished (or believed) they could escape the norms of general social, cultural, and legal discourse simply by designing ever more complex systems and protocols that "need" increasing levels of sensitive information to work. The lawyers come trooping in and write similarly complex terms and conditions and hope to paper over the problem or find a cozy loophole in unholy legislative agendas. Investors search in vain for beans to count. Everyone else finds privacy *boring* until their own self-interests are compromised.

At the same time, just as automotive technology eventually became a ubiquitous and necessary part of many more lives, so too has information technology, from phones to clouds, become such an essential part of industrialized nation-states. Personal data fuel and preserve the value of this new information boom. Thus, the technical elite no longer can dismiss the debate or pretend that data privacy doesn't matter, nor can they fail to build new creations that defy basic privacy precepts, which we will discuss herein, if they wish to see this new world unfold and grow.

If an executive at a global company publicly were to state that he doesn't believe in taxes and therefore will not pay them to any government, he would likely be removed or at least considered to be a great humorist. Not so for data privacy in the past. In the past decades, executives and other makers and consumers of information technologies regarded data privacy as some sort of religion that they could believe in or not at will and without earthly consequence. They certainly did not regard privacy as a *requirement* to measure, to debate in the boardroom, or to build at the workbench. We see these uninformed days of privacy as religion as nearly over. The age of data privacy as a set of design objects, requirements for engineering and quality measures, is dawning, and we hope to help the sun come shining in.

In fact, plain old-fashioned greed and an instinct for value creation will *hasten* the age of privacy engineering and quality. We know that the concept of privacy regarding one's person, reputation, and, ultimately, what can be known about the person has been the inspiration of law and policy on one hand, but we also know that innovation and the recognition that privacy—informational or physical—has value.

Andrew Grove, cofounder and former CEO of Intel Corporation, offered his thoughts on Internet privacy in an interview in 2000:

> *Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of when they called this the information age.*[4]

Thus, people living in the Information Age are faced with a dichotomy. They wish to be connected on a series of global, interconnected networks but they also wish to protect their privacy and to be left alone—sometimes. Both business and governmental enterprises, striving to provide a broad base of services to their user community, must ensure that personal information and confidential data related to it are protected. Those who create those systems with elegance, efficiency, and measurable components will profit and proliferate. History is on our side.

We call the book and our approach "privacy engineering" in recognition that the techniques used to design and build other types of purposefully architected systems can and should be deployed to build or repair systems that manage data related to human beings.

We could have similarly called the book "design principles for privacy" as the techniques and inspirations embraced by the design communities in informatics, critical design, and, of course, systems design are also a part of the basic premise where one can review an existing successful framework or standard and find inspiration and structure for building and innovation. The very nomenclature known as privacy engineering is left open to the possibility of further design.

The models shown are abstractions. Models are never the reality, but models and patterns help designers, stakeholders, and developers to better communicate and understand required reality.

Confidence in privacy protection will encourage trust that information collected from system users will be used correctly. This confidence will encourage investment in the enterprise and, in the case of charity enterprises, will encourage people to donate.

There are many books and papers on privacy. Some focus on privacy law, others on general privacy concepts. Some explain organizational or management techniques. This book is intended to be additive. This book crosses the boundaries of law, hardware design, software, architecture, and design (critical, aesthetic, and functional). This book challenges and teases philosophical debates but does not purport to solve or dissolve any of them. It discusses how to develop good functionalized privacy policies and shows recognized methodologies and modeling approaches adapted to solve privacy problems. We introduce creative privacy models and design approaches that are not technology specific nor jurisdiction specific. Our approach is adaptable to various technologies in various jurisdictions.

---

[4] "What I've Learned: Andy Grove," *Esquire*, May 1, 2000.

Simply put, this is a book of TinkerToy-like components[5] for those who would tinker, design, innovate, and create systems and functional interfaces that enhance data privacy with a sustainability that invites transparency and further innovation. We wish to demystify privacy laws and regulations and nuanced privacy concepts into concrete things that can be configured with flexible, engineered solutions.

The *Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value* is a unique book. We introduce privacy engineering as a discrete discipline or field of inquiry, and innovation may be defined as using engineering principles and processes to build controls and measures into processes, systems, components, and products that enable the authorized processing of personal information. We take you through developing privacy policy to system design and implementation to QA testing and privacy impact assessment and, finally, throughout the book, discussions on value.

- Chapter 1 discusses the evolution of information technology and the network and its impact on privacy.
- Chapter 2 discusses a series of definitions: policy, privacy engineering, personal information (PI), and the Fair Information Processing Principles (FIPPS).
- Chapter 3 covers data and privacy governance, including data governance, Generally Accepted Privacy Principles (GAPP), Privacy by Design (PbD), and other governance frameworks.
- Chapter 4 introduces a privacy engineering development structure, beginning with the enterprise goals and objectives, including privacy *objectives*, that are used to development privacy policy.
- Chapter 5 discusses privacy engineering requirements. We then introduce use cases and use-case metadata.
- Chapter 6 introduces enterprise architecture and the various views of it. We dig into the privacy engineering system engineering lifecycle methodology. We show the Unified Modeling Language (UML) usage flow from the context diagram, using the UML use-case diagram, to the use of business activity diagrams, including showing key data attributes, then on to data and class modeling using the UML class modeling diagram, and then to user interface design. We use the system activity diagram to show where FIPPS/GAPP requirements are satisfied within the privacy component design (scenario 1) and then we move to dynamic modeling where we define service components and supporting metadata, including the inclusion of privacy enabling technologies (PETs). We then discuss the completion of development, the development of test cases, and the system rollout.

[5]See www.retrothing.com/2006/12/the_tinkertoy_c.html for a random, cool TinkerToy creation by MIT students.

- Chapter 7 discusses the privacy component app, which will be used to maintain the Privacy Notice. The privacy team, along with the data stewards, will enter and maintain the privacy rules. When an embedding program requires personal information, the privacy component will ensure that the personal information is collected according to privacy policies.
- Chapter 8 presents, as an example, a small mobile app, using a simplified version of the privacy component to support a high school cross-country runners app.
- Chapter 9 covers an example vacation planner app that utilizes a privacy component that has already been developed, tested, and implemented by a large hospitality company that requires a system to help its customer community plan a vacation at one of their hospitality sites.
- Chapter 10 covers quality assurance throughout the development lifecycle, data quality, and privacy impact assessments (PIA).
- Chapter 11 discusses privacy awareness assessments and operational readiness planning.
- Chapter 12 covers the organizational aspects of privacy engineering and aligning a privacy function to IT, to data governance or data stewardship, and to the security management function.
- Chapter 13 discusses how data and data privacy may be valued.
- Chapter 14 covers our musings about the future of privacy and privacy engineering along with our Privacy Manifesto.

Why Anyone Should Care About Privacy, Privacy Engineering or Data at All

It's time to serve humanity.

> Humanity is people.
> Humanity is empowered stewardship of our surroundings—
> Our universe, planet, and future.
>
> Humanity is described by data;
> Data about humans;
> Data about all things human.
>
> Data is not humanity;
> Data tells a story;
>
> Data is leverage;
> Data is not power.

Humanity can capture data.
Data cannot capture humanity.

It's time to serve humanity.
There is no one else.
We are already past due.

This is the paradox in which the privacy engineer discovers, inspires, and innovates.
Let's begin.

PART 4

Where Do We Go from Here?

CHAPTER 13

Value and Metrics for Data Assets

It is the mark of an educated mind to rest satisfied with the degree of precision which the nature of the subject admits and not to seek exactness where only an approximation is possible

—Aristotle

Or, put another way, don't go over thinking things—or over measuring things.

—Steve Weiss, Editor

No precision is possible to quantify or qualify the value of data, well or poorly designed system efficiencies, or brand value if we fail to begin. Yet, the reality is that enterprises run on well-trod resources such as money, real estate, and property. They also run on brand loyalty, percentage of churn, customer satisfaction, and leverage. The point here is that it is hard to measure the value of intellectual or virtual property such as the right to use, process, or remain a fiduciary for data. This chapter will put forth some ideas and concepts about potential data or data-centric systems. A privacy engineer holding this book will recognize that, here too, is a topic rife with opportunity for quiet incremental improvement and bold innovation.

One of the most elusive, yet impactful, tasks before the privacy engineer is to find measurements for incremental progress in designing and executing data governance standards and utilities and to report those metrics in terms of value. Value may come in many forms:

- Qualitative value as in improved efficacy of data system flows and customer satisfaction
- Quantitative value in terms of:
  - Loss avoidance
  - Incremental gains in information-based products and services or those accelerated by PI
  - A lower percentage of churn
  - Lower perceived "creepiness"

It makes sense here to have a little refresher from a discussion we began in Chapter 2 that covered some of the differences among privacy, confidentiality, and security before addressing value and metrics directly. These differences are particularly interesting, as data privacy tools and models are built, differentiated, and measured for value creation among a thicket of security or general "compliance" goods and services.

Data privacy is, in a very real sense, the most immature of the categories of intellectual property (IP), even though its roots travel far back in time. Traditional notions of IP include patents, trademarks, copyright, trade dress, trade secrets, and the contractual or social concepts of confidentiality. Of course, these notions often offer up models of "ownership" or "control" beyond that comfortably conceived for data privacy and protecting information about humans, but the models are helpful when discussing or determining measurement or quantitative models deployed to arbitrarily value it.

Trademarks (and other IP analogous legal objects) designate the origin of a good or service. For better or worse, a trademark's social utility is to alert end users to the origin or owners, creators, or controllers of goods or services. As part of the exchange for a limited monopoly right to trade goods under an exclusive mark, the owner of the trademark has a bundle of rights and obligations (assets and liabilities) associated with such ownership. For example, under US law,[1] a trademark owner must police his mark to be sure consumers are not fooled into believing imposters' goods are masquerading as his own (the cost of these efforts may be viewed as an expense undertaken for securing or protecting the right to remain the sole source of goods). Similarly, an IP owner must also ensure that goods or services are of a consistent quality (another cost center or liability undertaken both to protect the asset and protect the consumer). On the balanced side of the economic valuation, a trademark owner is entitled to have a limited monopoly as the source of a good or service as a direct market advantage and is also entitled to gain an extra boost and intangible advantage as a greater brand strategy to build emotional or other customer equity.

Data privacy may be considered as the bundle of rights and obligations that arise from the data emanating from or describing a person. Whereas the trademark owner is the origin of the good or service, so too is the human an identifiable individual data subject the origin of personal information. Current laws, regulations, and culture create the obligations for those who wish to remain fiduciaries or processors of data, and those same contextual requirements also create a platform for opportunities for asset management and leverage.

There are a number of imperfect analogies and models to help guide the way to begin the measurement and evaluation of the asset and liability balance for data privacy. None are perfect, but they are a good start in the absence of existing practices. (Remember Aristotle: don't seek exactness when only approximation is possible.)

[1]In other countries, laws around IP differ much as they do for data protection as a reflection of local or regional custom and commerce. A trademark owner may, for example, be allowed to own a trademark for a certain period of time without proving commercial use of that mark or have differing rights in his ability to alienate his rights to the mark.

DO WE TREAT DATA AS ASSETS?

By Rena Mears, Managing Principal of RMCS, LLC

"We treat data as an asset . . ."

A ubiquitous phrase found in hundreds of thousands of online privacy policies[2] that succinctly conveys a sense of shared value and due care on the part of the enterprise to the web site user. Given its widespread use in privacy policies, it may be surprising to note that managing personal information as an asset is still in the very early stages of development within most enterprises. Many of the basic asset management processes such as inventorying, cost analysis, and asset valuation are in a nascent state, and consequently the tools and processes considered standard when managing other enterprise assets may be nonexistent or only minimally applied to personal information (PI) assets. So is it worth the effort and cost to develop these processes? Does adopting a more asset-based approach support or inhibit the effective and efficient management of personally identifiable information in the enterprise?

To answer that question, it is important to consider the definition of an asset, the various uses of PI in the organization, and the impact of valuation on the allocation of enterprise resources and shareholder value. The definition of an asset is deceptively simple:

- A resource controlled by an entity
- As a result of a past event
- From which future economic benefits are expected to flow to the entity[3]

However, when the criteria are applied to PI, the complexity of the management challenge becomes readily apparent. Diverse cultural, regulatory, and marketplace requirements have an enormous impact on defining and managing PI assets. Where, when, and how data is acquired ("past event") can determine what is considered a PI asset, how it can be used, and the level of control that must be exercised to effectively manage the asset throughout its lifecycle.

In response to this complexity, the general tendency has been to treat all PI assets as similar in nature and manage them on a tactical level as a cost-center issue. This approach often results in some or all of the following:

- PI asset management processes focus on risk reduction and cost minimization rather than asset optimization.

[2]Internet search results from "treat data as an asset" "privacy policies."
[3]International Accounting Standards Board. (2003). International financial reporting standards (IFRS's): Including international accounting standards (IAS's) and interpretations as at. London: International Accounting Standards Board. Elements of financial statements (IAS 1 article 10)

- Senior management involvement is limited to crisis response (e.g., breach, regulatory, enforcement action) or periodic reporting of risk (e.g., changing law, audit findings) and does not extend to consideration of strategies to maximize return on the PI assets.
- Managing PI assets defaults to the midmanagement layer of the organization and is treated primarily as a legal and compliance issue.
- PI assets are maintained in silos and management may be inconsistent and unaligned with company strategy.
- Enterprise resources (e.g., budget, human capital, technologies) are allocated evenly across all PI assets regardless of the value of individual assets, resulting in misallocation of resources, hidden costs, and unnecessary expense.
- Inventory of PI assets is incomplete or nonexistent, thereby limiting management's ability to evaluate, manage, and optimize the asset.

Changing market conditions are forcing a reexamination of this cost-based approach to managing PI assets. Companies that once considered themselves solely product oriented now see themselves as "information-driven" businesses that rely on data assets, including PI assets, to compete effectively in the marketplace. Innovative technologies and reduced storage costs support the acquisition and mining of vast amounts of data. The rapidly expanding definition and changing role of PI assets in current business models is driving the need for a more nuanced approach to evaluating and managing these assets.

A utility-based approach to asset management examines the "usefulness" or net contribution of individual or subclasses of PI assets to the value chain of an organization. The approach considers the various use cases of PI assets to identify future economic benefits (e.g., revenues, product enhancement), associated costs, and potential risks to determine net contribution values. Assets with similar use cases, characteristics, and values may be grouped into asset profiles that form the basis for asset optimization through strategy development and the application of customized management processes. It is important to note that asset optimization of PI assets is not the same as merely maximizing direct revenue from the use of personal information. There are many use cases for PI assets, and enterprise utility may relate to support activities and contributions through risk or cost reduction (e.g., meeting legal requirements, optimizing talent acquisition). Some advantages that may be expected when adopting a utility-based approach to PI asset management are:

- PI asset management approach focuses more broadly on asset optimization and considers opportunities and risks beyond legal and compliance requirements.
- Senior management involvement extends to the development of PI asset strategies and supports enterprise recognition of the strategic value of PI assets.

- Management of PI is appropriately positioned at all levels in the organization, resulting in more efficient use and effective control of the asset.
- Enterprise resources (e.g., budget, human capital, technologies) are allocated in a more "value-based" manner, thereby focusing expenditures on assets with the highest contribution to the enterprise value chain.
- Basic asset lifecycle processes (e.g., inventorying, cost analysis) are applied to PI assets and may result in identification of new management options (e.g., "build or buy," outsourcing).
- Underperforming assets can be identified and managed appropriately (e.g., retired or deleted, access/use limitation).

Many organizations consider it too costly and very difficult to adopt a utility-based approach to PI asset management. However, the cost of not adopting such an approach may mean that PI assets continue to be treated as "white noise" in the enterprise, widely distributed throughout the organization and relatively homogeneous in nature. That approach ignores the very essence of the definition of an asset and will likely ensure that PI continues to be a source of high risk, hidden cost, and unnecessary expense to the enterprise. Suboptimized assets whose risks and cost outweigh their contributions are more commonly known as liabilities.

Finding Values for Data

> *Some day, on the corporate balance sheet, there will be an entry which reads, "Information"; for in most cases, the information is more valuable than the hardware which processes it.*
>
> —Rear Admiral Grace Murray Hopper

Values for data protection measures have been based on survey and anecdotal evidence relating to reported data breaches. Such breach reporting is typically thrust upon an enterprise by prevailing data breach legislation, best practices relating to credit monitoring or other services, and legal or marketing expenses undertaken in response to the negative perceptions caused by such breaches.[4] Another method for measurement

[4] "Ponemon study shows the cost of a data breach continues to increase." www.ponemon.org/news-2/23

may be to analyze prior fines or other regulatory requirements, such as Federal Trade Commission Consent decrees requiring as much as 20 years' oversight by a third-party audit company or other self-reporting mechanism.[5]

These traditional methods for data valuation fall short of the hoped for objective in a few fundamental ways. First, they are retrospective and often based on internal process or insider bad action—often quite difficult for an enterprise to anticipate or prevent. The incident may have arisen from a criminal actor, such as a hacker, or from product vulnerability in an increasingly complex IT ecosystem.[6] Second, the cost of a failure is but one component of risk avoidance—inefficiency, uncurated data mismanagement and waste, and, most important, true data asset prospective value are rarely addressed and even more rarely managed as sources of proactive investment.

Uncurated data is data that is not assigned to, owned by, or governed through specific methodologies or specific responsibilities. In short, this is data that is not being actively processed or organized to add value to either the data subject or the enterprise. For example, special events and business conferences require a great deal of personal data to accept payment, organize meetings, arrange travel, and more. Some of that data remains and grows in value as it is leveraged to build relationships with participants and personalize goods or services while the same data poses a risk only if left neglected or unused for its intended purpose.

Some data loses its relevance and becomes a compliance liability or risk where the data directly related to ended events or meetings for logistics, for example, is no longer needed for any relevant conference-related purpose. Retaining irrelevant portions of collected materials (or information) costs an enterprise money, time, and other resource expenditures. Although hardware storage may seem inexpensive and the myth persists that retention of data past its original purpose may create a "what if" or potential asset value, such is rarely the case. In fact, an enterprise may not have the legal right to process uncurated data if the future purpose of processing is beyond the original purpose.[7]

A mental experiment is helpful here, where a CFO continues to pay to store and move a warehouse filled with notebooks and pencils. These office supplies may be useful for future meetings or for scratch paper if date embossed. Nonetheless, if no one understands where the warehouse is located, if it has doors or a lock, and the nature of the supplies, and if no one has any responsibility for the warehouse's content,

---

[5]There are many examples of FTC Consent decrees and Data Privacy Authority sanctions with a variety of financial or other equitable remedies. In many countries, sanctions are either fines or undertakings to alter activities. In the United States, most federal-level penalties also contain the obligation for an enterprise to pay for annual audits of the enterprise privacy compliance efforts. See Microsoft's consent decree settling allegations with the FTC that the company made false statements regarding its ability to provide privacy or security to its customers. www.ftc.gov/opa/2002/08/microsoft.shtm. See also France's Commission nationale de l'informatique et des libertés (CNIL) sanctions against Google and its specific requirements that it hopes to impose on Google for its processing of French PI. www.cnil.fr/english/news-and-events/news/article/google-failure-to-comply-before-deadline-set-in-the-enforcement-notice/

[6]See "Predicting the unpredictable: Detecting chaos in mathematical equations." www.mit.edu/newsoffice/1998/chaos.html

[7]See OECD Guidelines Purpose Principle, discussed in Chapter 2.

the enterprise must continue to pay for its management, realizing no further value and risking further losses by fire or workplace injury for movers or other unexpected problems. Just as the information ecosphere provides the potential for massive data stores and assets, so too does it create the very real possibility for waste, loss, and unplanned risk.

KNOWLEDGE GOVERNANCE

By Kenneth P. Mortensen, Chief Governance Officer at CVS Caremark

> *What is a system? A system is a network of interdependent components that work together to try to accomplish the aim of the system. A system must have an aim. Without an aim, there is no system. The aim of the system must be clear to everyone in the system. The aim must include plans for the future. The aim is a value judgment.*
>
> —Dr. W. Edwards Deming,
> *The New Economics for Industry, Government, Education*

In the age of "big data" and "advanced persistent threats," a privacy professional can no longer focus solely on developing and implementing the processes and procedures to drive information governance, but rather she needs to advance her organization through the optimization of risk while facilitating core management decision making in order to create real value. This is the new world of "knowledge governance."

In the past, an organization looked simply to corral its data into a warehouse so that it could be understood which datasets and which data elements provided operational leverage within the activities or functions of the organization—otherwise known as "data governance." By producing a common or uniform view into the organization's data, data governance allowed, for the first time, an understanding of which data fed the organization's activities or functions. Nevertheless, this was a single dimension view that lacked the ability to understand the utility of the data within those activities and functions. Without a view to the data utility, an organization flies blind to legal and regulatory compliance issues, such as with privacy and information security. Thus just having a common understanding or reference model for the data of an organization does not open up those data for use and disclosure without significant risk regarding privacy and security.

From that gap, the privacy profession promoted the concept of "information governance" that allows for the data to communicate information. In literal etymological terms, information means to give form to something. In business terms, the word focuses on the ability to transmit data by providing form to a message by casting it into a profile or pattern for communication (sharing). This means definitions for information can be grouped roughly into quantitative and qualitative categories.

The qualitative definitions focus on the criteria that add meaning to the message that is communicated. The quantitative definitions focus on measuring the quantity of information units or the strength of its transmission. But this alone did not address the risks inherent with data governance. The governance aspect at the information level comes from the effective and efficient management of information within organizations. Management is the process of getting activities completed efficiently and effectively through the enterprise. The goal (or function) of management is to get the best return on enterprise resources by getting things done efficiently.

There are four basic pillars to any management process: plan, organize, direct, and monitor. An organization must, through data governance programs, *plan* the path for information within any organization as well as address any external collection or disclosure. Next, the organization will need to *organize* not only the data, which gets the organization only as far as data governance, but also the uses and disclosure to discover the utility of the information. From those uses and disclosures, the organization can *direct* protections and safeguards so that the organization can not only use the information thoroughly, but also in a compliant manner. Last, the *monitoring* of the processes and procedures is crucial to ensure that governance works to drive continuous compliance.

At this point, many organizations put down their tools, convinced that they have full use of their information in a methodology that ensures compliance with needed privacy protections and necessary security safeguards.

Unfortunately, these organizations, while able to survive the enforcement environments because they operate in a compliant manner, cannot progress into having full enterprise understandings of what value they can extract from all the information. Legal compliance does not optimize risk to the organization; nor does this coordination of effort address more than one facet of risk. The organization must look to all functionalities of the organization to understand the impact of risks associated with the information resources. To move to the next level and attain "knowledge," the organization must address information and its management strategically. Strategic management of information across the organization addresses not only the need to optimize the risk to the organization, but by establishing all the information as a critical organizational (or, better put, *enterprise*) asset, if not the most critical asset, the organization can introduce effective efficiencies into the decision-making processes for management, enhancing the return on the investment in information. An organization needs wide-ranging processes to capture not only data protection, but also data compliance, which takes in the complexity and diversity of the risk and legal environments. Knowledge is the value form of information, just as information is the communicative form of data. To accomplish this objective, an organization must employ enterprise governance that addresses all aspects of information within the organization with processes and procedures to deconflict and reconcile priorities to ensure governance efficiency.

Once knowledge governance has been achieved, an organization can extract the value of core data and information. The organization's leadership will be guided by this knowledge in advancing the goals and objectives of the organization, or as Dr. Deming noted when addressing similar issues from a quality management aspect:

> *The prevailing style of management must undergo transformation. A system cannot understand itself. The transformation requires a view from outside. The aim . . . is to provide an outside view—a lens—that I call a system of profound knowledge. It provides a map of theory by which to understand the organizations that we work in.*[8]

Knowledge governance for data assets can only be enhanced by further exploring other metric and valuation models. As is true for other sections of **The Privacy Engineering Manifesto**, methodologies and processes have been undertaken to create useful valuations of difficult-to-measure tangible and intangible inputs and outcomes. Data privacy is neither the most unique problem in the world nor the least measurable. Nonetheless, to quote the late American novelist David Foster Wallace, sometimes "the most obvious, ubiquitous, important realities are often the ones that are hardest to see and talk about."[9] Once discovered, the language of value for data privacy may be the key to opening the door to more practical matters.

Valuation Models

The following potential models should be viewed as a sketch pad of sorts; a group of potential techniques and tactics for assigning values or making concrete the value for data and data-centric systems. As technologies become more deliberately designed for data protection and policies evolve to become both legally more efficient and compatible with requirements setting, so too should valuation models evolve.

Model 1

Find something to count and count it:

- Data breach, customer churn after direct enterprise activity, or other regionally relevant contextual activity (such as a significant breach or a news-making threat or economic instability that causes data or customer contacts to increase or decrease).
- Leverage the GAPP maturity model and gauge costs to move to a higher maturity model. Balance cost against brand valuation, data reliant programs, or marketing events to the percentage spent to acquire customers.

[8] W. Edwards Deming, The New Economics for Industry, Government, Education, Ch. 4 (1994)
[9] "This is Water", Commencement Speech to Kenyon College class of 2005 written by David Foster Wallace.

- Read 10K annual reports or other publicly available, legally binding documents to find data-critical programs such as expansions into new jurisdictions, outsourcing, or cloud shifting business models or determine the geographic mix of customer or employees who provide critical data to the enterprise. Make an educated or sample-based guess regarding the importance of employee or customer data access based on these disclosures.
- Estimate IT spent regarding data-centric systems, and measure the cost of management and governance for technology in terms of full-time employees headcount's, legal, or other professional services or audit requirements (i.e., How much do the systems, processes, and technologies that process personal data cost?).

Model 2

Track time to deployment or proof of concept in a privacy engineering instance vs. traditional deployment. Start and track improvements in development, speed to deal closure, or other processes to attempt to measure organizational efficiencies.

Model 3

Work within the grain of cyber insurance. An enterprise will only be covered by cyber insurance where certain conditions are met to prove that the enterprise has taken at least reasonable steps to prevent loss. Create a checklist for coverage for various relevant scenarios based on the current level of cyber coverage or similar coverage within a relevant industry or size of enterprise for incidents such as hacker or other criminal external compromise, advanced persistent threat (APT) exploitation, negligent loss of media device, or physical encroachment. Generate the cost of repair or staffing to attain reasonable coverage in the event of a cyber incident.

Model 4

Look for qualitative or reputational examples rather than numerical values. For example, there are tools and techniques leveraging other individual's expressed curiosity, socially networked assertions, or trends according to big datasets or other analytics that can show relevance to the enterprise and value to individual customers.

Model 5

Leverage the known unknowns of brand valuation. Brand value determination is calculated using certain evidential or inferential techniques. Roughly stated, brand is measured as the difference between book value (adding all countable assets such as real estate and improvements, manufacturing assets, and the combination of financial assets relating to currency and investments) and market capitalization value. Where there is

a market and that market decides that a company is worth more than tangible assets, that differential is the collection of intangibles, potentials, and connective tissue that ties customers and employees to an enterprise and allows investors to decide an enterprise's potential.

PRIVACY IN THE ERA OF THE DATA ECONOMY

Chenxi Wang, Ph.D. Vice President of Market Insights at McAfee

We are living in the era of the data economy. The advent of consumer mobility and social media gave rise to a massive amount of readily available data to mine, aggregate, share, and analyze. IDC estimates that by 2020, there will be "40 zettabytes of information in the digital universe".[10] What's more, the composition of data products and applications can lead to brand new business models and previously impossible value propositions : consider Uber (the private, on-demand car service) in a world without Google maps.

Modern businesses now understand that access to data equals power and competitive advantages , and there is an increasingly large appetite to collect, store, and mind data. It is entirely possible that soon we will see a global market where data products and applications are routinely traded and exchanged. This trend has led to data obesity, heightened risk for data misuse, and an increasing concern for the threat to privacy.

Just like any other market, the data economy is governed by supply-and-demand and a value/pricing framework. Privacy regulations, however, typically seek to govern the supply and demand relationships, while completely ignoring the value framework. We argue that privacy is not attainable unless the value/pricing framework takes privacy impact into consideration. In other words, the value assessment of the data should not be solely based on their potential for creating valuable data products, but also based on their potential exposure to privacy risks.

Consider, for example, the case of a patron entering a bar. To gain admittance, today the patron needs to show her driver license, which discloses his date of birth, weight, height, and home address. Much of this information is beyond what the bar needs to know to permit entrance to the premises.

Consider again the same case when the patron approaches the bar, she is presented with three options: a) minimum disclosure to gain entrance (i.e., prove that she is over 21, the legal drinking age), b) disclose demographic information (i.e., age, gender) for a drink coupon, and c) consent for location tracking and ad serving for a much larger drink coupon.

[10]IDC's latest Digital Universe Report, released in December 2012, estimates that the amount of digital data produced will exceed 40 Zettabytes by 2020. This assumes all data is expected to double every two years.

If the patron chooses option A, her picture will be taken and sent to an information cloud for age verification. The answer that comes back from the cloud will be either a "yes (over 21)" or a "no (below 21)" , with no additional information such as date of birth. The picture is then deleted and the patron gains access to the premises.

If the patron chooses option B, the information cloud would disclose, along with age verification, demographic information such as age group, gender, etc. This information will be used in the bar operator's data mining and marketing efforts.

If the patron chooses option C, she would be asked to download an ad-serving app, which serves her relevant ads based on her location and activities.

Of course there could be other levels of information disclosure, but let's look at what just happened in the above scenario:

First, the customer has all the control: she can decide how much information to disclose.

Second, the marketers are not completely ignored here: they can get opt-in information, for a price.

The minimum disclosure is contextual: here the information disclosed is whether the user is above or below 21 years of age, but in other cases minimal disclosure can be about other data that make sense in the specific context of the activity. For example, location for local Yelp services may make sense in context.

There is a trusted intermediary—the info cloud in the example—that brokers the data exchange. The data broker does not have to be a singular party, but it needs to be a public entity trusted by the data owner.

To make this a reality, we need to establish a data value framework and a new model for the data supply chain. The data supply chain should include the designation of authoritative data suppliers, an access authorization model, authentication, data aggregation models, etc. The work done by UMA, for instance, is an example of an user-centric authorization model.[11]

The data value framework is arguably the most interesting, because it denotes how data will be assessed and traded, which are fundamental elements of an economy. One can consider a rudimentary value framework as follows: Pick your favorite data taxonomy, order the categories based on their exposure to privacy risks (if possible), and price them accordingly (the higher the risk, the higher the price tag). Afterwards, for each user-authorized data access, if the data required fall into minimal disclosure, they are supplied free of charge. Outside minimal disclosure, the data are

[11]UMA: User Managed Access (UMA) is an industry working group that is developing specifications that will allow an individual to control the authorization of data sharing and service access made between online services on the individual's behalf.

supplied with the attached price. For those data items that the user does not wish to grant third party access, the price tag can be set to infinite.

Clearly there are many options and intricacies to data value assessment beyond this basic framework. For example, how do you handle derived data, those that only exist based on previous data accesses? Similarly, the issue of what is considered minimal disclosure can be debatable.

However, we argue that without such a contextual data value model, either consumer privacy or the increasingly flourishing economy built on data sharing will be undermined. Businesses who truly understand the business impact of data and adopt this privacy-embedded data value framework will see consumers as willing participants in the data economy, where data exchanges are contextually relevant, properly priced, and in a manner that respects their privacy.

So, in many ways, the formula under a brand-based methodology could be that "brand" is the superset where intellectual property (IP) plus personal information (PI) are significant subsets of that market-driven asset. It is also illustrative that countries such as the United Kingdom, France, Australia, and New Zealand allow for intangibles to be included as part of an enterprise's balance sheet.

Brand values have been used to defend against a hostile takeover, as an investor relations tool, and, sometimes, as a performance indicator for the long-term investor. International standards that allow for intangible values may be leveraged and borrowed to assist in documenting PI value for the privacy engineer. For example, the International Accounting Standards Board (IAS 38), UK Accounting Standards (FRS 10 & 11), and US Accounting Standards Board (FASB 141 & 142 under Generally Accepted Accounting Principles) all may be used to determine or infer acquired goodwill. If the analogy from brand value to a subset of PI plus IP value is to be considered, it should be carefully noted and considered that the concept of "impairment"—roughly, the extent to which the stated value does not reach market value for a market-based enterprise—also impacts the PI value.

Here, the process and practice of privacy engineering becomes conceptually very interesting. Part of the controversial nature of valuing intangible assets is where those assets defy measurement. Compliance for data protection measures can be similarly difficult to achieve where enterprise governance professionals are unaware where data reside and how it is actually processed, and they do not have a means with which to measure processing over time. Where privacy engineering practices are followed, data is managed from its earliest analysis, design, and instantiation throughout its lifecycle. In such systems, active management and impairments based on market perception or active risk taking using data assets can be known and tested.[12]

[12]For example: www.nysscpa.org/cpajournal/2002/0202/features/202fp.22.htm

PRIVACY MATTERS BLOG SERIES: QUANTIFYING REPUTATIONAL RISK[13]

By Michelle Finneran Dennedy, published on Jan 06, 2012

There are many kinds of risk: operational, legal, and reputational risk. Most large enterprise IT teams are comfortable and proficient at measuring operational risk. It features in reports as minutes of downtime, incidents of endpoint reimages, number of patches installed, hours of overtime.

Legal risk isn't that hard to handle, either. IT can draw on peers, auditors, and legal staff for expertise.

However, reputational risk seems to be a far more unfriendly concept. I find technical people typically consider reputation a soft science, a squishy topic that can't be measured. As a result, IT can't set goals, gauge progress, or claim success based upon "reputation," and product creators cannot specify requirements for "reputation." Because it can't be managed like other metrics, IT staff and technical business units may ignore or downplay reputational risk's potential impact on the business—and their roles in protecting it.

IT is Missing a Gigantic Opportunity

I believe you *can* measure—or at least approximate—reputation, applying metrics to the same influences that affect your customers and your C-Suite executives: news headlines and stock prices. If you count the number of published, reputation-buffeting events each month—the headlines in the email news summaries you receive from SC Magazine, for example—you can see what the public is talking about, and that dialog will affect the rise and fall of organizational stock prices. Reputation and market sentiment are huge factors in market valuation, which is something your CMO and CFO are tracking. Although your interest may be in the technical security side of the business, you can take actions to measure, manage, or mitigate reputational risk.

Building a Reputational Heat Map

Well before the mortgage crisis was discussed in the public and mainstream press, it was anticipated in whispers at investment community conferences and insider blogs. Eventually, and much too late for most people and the economy, it was covered in USA Today and other mainstream papers on the doormats of hotel rooms coast to coast.

[13]This blog entry is reprinted in its entirety from McAfee's external web site: http://blogs.mcafee.com/business/security-connected/privacy-matters

Security issues that affect risk appear first in smaller, insider places, too. Then they migrate to the mainstream, to NPR, the Washington Post, Wired, and Vanity Fair. (Look at Stuxnet references on Wikipedia for a great example of this sequence.) With enough mainstream angst, trends start to register on the regulatory radar—with the European Community, the Federal Trade Commission, and others. We experienced this pattern with behavioral marketing. Privacy advocates raised objections in 2005, well before the FTC published its principles for behavioral marketing in December 2007. We are still seeing news and blog coverage on this topic today as companies experiment and push the envelope leveraging new technologies and relationships.

By the time a security topic attracts a reporter in the mainstream press, you had better have a strategy for that problem. You should be able to brief your boss with an assessment of your business's risk, including the risk to your reputation.

This assessment is possible, but you need to be selective. Just as you don't want to read every log entry from your IPS, you don't want to attempt to assess all topics everywhere on the Net. Instead, think about YOUR audience and what they read—or you wish they would read. Look at two tiers of publications: mainstream media and online influencers, including blogs and news feeds. Sign up for emailed daily updates if they are available from the 3–5 most relevant sources. Also, if there is an "insider" conference, you can look at the session titles and monitor news summaries for perspective on what the industry thinks is hot.

Next, think about what risks would affect your business and its reputation. The tech bloggers today might be talking about SQL injection, advertising dollars, identity theft, or phishing. What is newsworthy for your audience? Would a successful hack at a competitor raise questions about your security? Would regulation banning use of cookies affect your service offerings? If yes, use these ideas to set up RSS feeds.

That's your pre-work. You should revisit these decisions at least once a year, or when your business or the markets change significantly.

Now, the ongoing process. Your workflow is to:

Notice topics that relate to your risks.

Count the number of times these topics are mentioned in headlines or news stories. Depending on your work style (and the frequency of the publications you are tracking), you might either jot down mentions as you see them or save these mentions in a file for review monthly.

Create a spreadsheet: rows are the topics, columns are the dates. In each cell, note the number of headlines or significant mentions. If you think it's going to be important, start to capture dates and publications (use links if you can) so you can back up your ideas. (Store this info somewhere else, not in the mention count cell, or you won't be able to convert to a chart.)

> Once a month, use the spreadsheet's charting function to generate a "heat map," an assessment of which topics have generated the most energy in the news.
>
> If a relevant topic has generated significant coverage in insider publications, there's a good chance it will reach the mainstream press. If you think this might happen, summarize your findings in a concise note to your boss and your security team. Include an overview of what the issue is, what the coverage has been so far, what the impact would be on your business, and what efforts might be appropriate to mitigate these risks.

Voila.[14] You have quantified reputational risk.

Do this well, and you will be prepared if and when you need to discuss ideas with others. Instead of coming in with only technical data about a problem, you can talk with your colleagues in the context of the risk landscape. You look more strategic and more business-oriented. You are doing more, considering more, and recommending risk management efforts that are proportional to security. This position supports IT's increasing need to do internal selling to non-IT people in order to get the right projects funded.

At a minimum, this exercise will keep your knowledge of the risk landscape current, and you will be more fun at parties. You can talk to non-security people about ideas that they will recognize and explain risks in terms that they can understand. Perhaps you will detect the next "mortgage crisis" level event in time to help a few people avoid its devastation.

Building the Business Case

Measurements are only science projects until they are leveraged for positive progress. A privacy engineer's innovation can be lost without a market into which to sell the goods and services created with these methodologies or, similarly, it can be lost where internal enterprise measures are not sustained for continued improvement that results in better knowledge governance.

One approach is to treat privacy engineering products, services, and processes as *intrapreneurial* opportunities. An *intrapreneur* is an innovator within an enterprise who takes on the responsibilities for creating and "selling" new techniques or even new privacy business units. To become successful, intrapreneurial teams must connect with executive and operational teams to fit new things into existing environments effectively.

[14] Okay, so nothing is that easy, particularly in the world of data privacy and security, but hyperbole is a gimmick and the "voila" was a dead giveaway that I was trying to be dramatic for effect.

For example, when talking to the C-Suite:

- They hate details
- They don't know about detailed data privacy laws
- They hate details
- They have never seen a data valuation model, but they do like cost/benefit analysis where benefits are costed out realistically and the cost side looks real
- They hate details

PERVASIVE RISK MANAGEMENT APPROACH FOR EFFECTIVE PRIVACY ENGINEERING

By Vidya Phalke, Chief Technology Officer , MetricStream

A comprehensive and sustained risk management program is critical for an enterprise's long-term sustainability and predictability. Risk management needs to be comprehensive across all facets of operational, financial, legal, regulatory, reputational, data security, and intellectual property risks. In addition, it needs to permeate into an organization in a *pervasive* and deep fashion. The basic recipe for this pervasive treatment of governance, risk, and compliance is created by putting together models—both qualitative as well as quantitative—so that decision makers in an enterprise can create a deep understanding of their risks and then use that understanding effectively for planning and managing the short- as well as the long-term objectives at each level of the organization.

Although pervasive risk management is a broader topic, I will use this book's privacy focus to describe a mechanism by which a quantitative model can be orchestrated that will help management of risk that is based on how well privacy risk is understood and managed. This same mechanism can then be extrapolated for other areas of risks to arrive at a pervasive risk management architecture.

Whether it is government agencies or private organizations like banks, insurance companies, or health care providers, the need for incorporating privacy protection and managing privacy risk is not only a regulatory and legal obligation but it also has to be part of the risk management plan. The first step in tackling this risk is to create a comprehensive list of enterprise-wide assets and processes and map them to their privacy risk. This exercise typically is done in conjunction with IT and various functional units. If an enterprise already has a risk or compliance office, then that is usually a good place to start.

Second, a comprehensive assessment across all these assets and processes should be done along the dimension of privacy from a risk as well as a regulatory standpoint. If that has been done already, then that assessment can be leveraged.

The key here is to look for *privacy component* capabilities as described in this book in each of the assets and processes. In addition to looking for those components or their surrogates, a review of past audits, control or compliance testing, industry events or incidents, and other management evidence needs to be taken into account as well. Remember, this assessment needs to be wrapped into overall change management processes and frameworks.

Typically risks due to privacy issues will flow into both legal and regulatory risk as well as reputational risk, and assessment of the likelihood and impact has to be done based on qualitative and quantitative factors followed by evaluation of mitigating controls. As discussed in this book, the assessment need not be extremely precise but can start with an approximation. For example, measuring the privacy controls and usage of privacy components (or lack thereof) can lead to a score ranging from 0 to 5. These scores multiplied by the value of the asset or process they are tied to creates a weighted risk score. The process of assigning value to an asset or process in an enterprise is a well-defined science, so I will not spend time on that here; however, it suffices to state that it is tied to business criticality, footprint, and extent of being proprietary. For example, a database that contains PI that is accessible to an outsourced data analysis company will have a much higher footprint weight as compared to one that is accessible to a fixed known set of data analysts that are internal employees of that company. Once the comprehensive asset and process privacy risk assessments are computed, they need to be multiplied by the organizational weight of that business unit or functional division and then rolled into a score visible to the senior management.

Once this quantitative framework for risk management is put together, the next important aspect is to ensure that it is brought under the umbrella of enterprise change management; this is critical to ensure that as changes happen and new information is discovered, the impact of those changes is captured in the risk management framework. For example, in the above case of a database with PI, if a new application is being brought in that will be integrated within this database and will expose the data to a bigger set of users, then the risk parameters need to be reassessed and appropriate mitigation and controls need to be updated.

Figure 13-1 presents a pictorial summarization of this architecture and flow that should be applied to assets and processes to build a pervasive risk management framework and system.

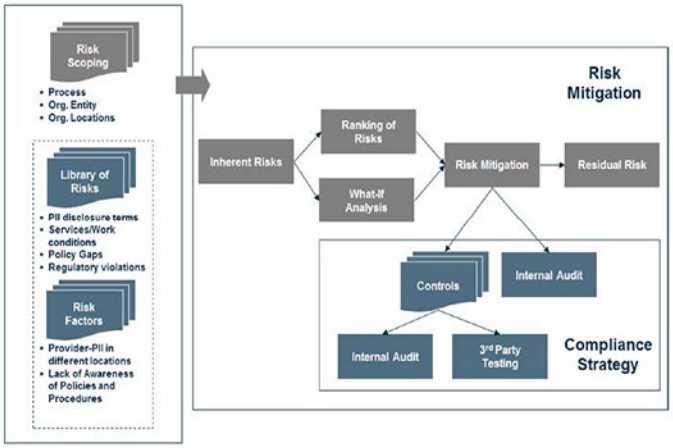


Figure 13-1. *Risk management with privacy use case*

Turning Talk into Action

Allies and other enterprise sponsors can help add to value models and create momentum. Privacy engineers *must* find allies such as the CFO, auditor, CMO, CTO, or any other leader willing to innovate with them and take on a bit of personal credibility risk. New things such as data valuation models can be perceived as unnecessary or not impactful or already managed by audit committees or compliance teams. Innovation in valuation models may require as many facts being marshaled from various measurement techniques as possible before a persuasive technique is selected for the enterprise.

Conclusion

The word "privacy" creates a marketing challenge. The paradox for creating data value models and systems can begin with this marketing issue. If enterprise stakeholders do not perceive or measure data risks and opportunities, they may well fall into a common trap. They may falsely assume that there is no need for privacy (after all, everyone says so). Another false assumption, if they do understand data about people or data derivatives have value, true stakeholders may feel that "someone else" owns or is accountable for the issue. Both false assumptions also suppose that data value is a thing or a static object as opposed to a flow, as is the case in capital- or currency-based value systems.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR JONES FROM JEFFREY RITTER

Discrimination

Q.1. In the Banking Committee, we often discuss discrimination involving loans and housing. As technology helps companies become more sophisticated it is easier to put in place discriminatory policies. Are there are protections currently in place that prevent data discrimination by race, gender, or religion? If not, what methods should Congress consider to decrease discrimination within data?

A.1. Discrimination of any nature, whether by machine or by human conduct, is the result of two actions. First, an individual or class is assigned a classification. It does not matter if that assignment is accurate; what matters is that the classification is paired or linked to the individual or class. Second, rules are constructed, and applied, which differentiate between classes in the allocation or availability of benefits or the imposition of sanctions.

When business is conducted through machines, both of these actions require specific inputs. A classification scheme must be composed, and the rules must be authored to expressly rely upon the classification scheme. Both the scheme and the rules must be inputted into the machine in order for any application or process to execute consistently with the scheme and the rules.

To prevent discrimination, I suggest the key is to prohibit the use of classification schemes and, in turn, prevent those schemes being used to associate a classification with an individual or class. It is not sufficient to prohibit discrimination; Congress must enable regulators to be able to inspect the operating systems of those companies and financial institutions within their purview and affirmatively confirm the absence of the classification schemes or their connections to individuals or classes.

Of course, if any institution wishes to establish and administer discriminatory policies, and not be caught doing so, then either the scheme or the rules can be cleverly designed. As just one example, rather than discriminate explicitly based on race, ZIP Codes or housing locations were historically introduced as a classification scheme that was not expressly racial, but still advanced the intended policies of those seeking to discriminate.

Therefore, diligence will be required from the regulators to also evaluate the relevant rules. Unfortunately, discriminatory rules will often be embedded into decision algorithms that require competent analysis to both recognize and sanction inappropriate rules. Therefore, Congress must authorize suitable funding to both recruit, train, and support competent professionals capable of conducting the required analysis.

Whether we like it or not, effective nondiscrimination regulatory frameworks in the 21st century will require increased transparency

and real-time availability of the operating data of regulated entities to regulators. While much progress has been made, particularly in SEC-regulated areas, toward those outcomes, Congress must recognize that nondiscrimination regulatory frameworks will not be effective without increased transparency and real-time data availability.

Given the global nature of competition, the United States must recognize that limiting governmental oversight of financial institutions will impair their trustworthiness in larger markets, handicapping both their strength in entering new non-U.S. markets, as well as attracting and retaining customers within the United States who increasingly find the stronger privacy-based oversights under which foreign institutions operate to be more appealing.

Data Privacy

Q.2. So much of data privacy is having the choice to share information. For example, many people find targeted ads to be disturbing and others find it serves as a helpful reminder. How should policymakers consider different preferences as they write legislation on personal data privacy and how it is used?

Many services require information from one site to be shared to another in order for the consumer to have access to the website's services. Sometimes this information sharing is helpful and makes the website more user friendly, but sometimes the data shared does not have any obvious benefits to the consumer.

A.2. In my oral statement and written testimony, I advocated for the principle that we must answer the question: who owns data information? During the hearing, we did not address the many technology innovations which are advancing (and, most notably, almost without exception, outside the United States) that allow individuals greater exercise of control over their data. "Control" is the digital equivalent of "possession" (as in "possession is $^{9}/_{10}{}^{th}$ of the law") and, by enabling individuals to gain control of their data, they are aligning themselves with the essential basis for ownership to be asserted. And, in doing so, the individual can then better assert and exert their preferences on the use of their personal information.

To date, individuals have enabled the collection, use and sharing of their information without much protest. But the real deficiency has been the absence of the technologies that allow the individual to exercise their control.

While in many instances, such as a patient arriving at a hospital in an ambulance, data ownership is not relevant to securing the appropriate medical care. But in commercial engagements such as those involving data sharing between different companies to gain access, having the technologies to exercise control will be vital and appropriate for use.

Rather than attempting to regulate specific preferences, consumers may or may not assert, I urge Congress to put in place the regulatory foundation for enabling consumers to own their information and, in turn, exercise the appropriate controls on how that data can be used.

Q.3. I am concerned that Congress will enact data privacy legislation but then websites will deny access to consumers for simply not

approving sharing their data. Should consumers be denied access for not approving data sharing?

A.3. This is an entirely appropriate concern but one for which I strongly believe there is no basis.

In the 21st century, data is becoming a different type of currency. In virtually every transaction, whether commercial or consumer-oriented, the "buyer" and "seller" are negotiating to establish equivalent value for what each is offering to the other. Since data is a new kind of property, it has become part of that valuation discussion. So, moving forward any transaction involves calculating the values for goods, services (such as access to a website), money, and data.

If a business conditions access on a consent to data sharing, that is just one variable that the consumer can consider. The great thing about the internet is its capacity to foster competitive alternatives. While we view the big tech companies as big, we overlook how well competitive alternatives (such as Alibaba in China) developed. So, if consumers have options on how to access web-based services, where a competitor may offer different "terms" for data sharing, that is a tremendous, positive outcome.

Indeed, I would encourage companies that wish to condition access on data sharing to do so, in order to foster the environment where competition can arise.

From the consumer side, as anticipated in the proposed California regulations, it is also possible to imagine that additional incentives might be offered to secure the consent of a consumer to share their data—such as discounts, coupons, or added services. Wouldn't it be great if consumers had choices in which their "price-shopping" among competitors might also include comparing the relevant values being offered to enable data sharing.

If the overall value of access is "worth" data sharing, that is entirely acceptable in my opinion. But its critical to make the affirmative decision to share part of the negotiation—unlike today's environment. Alternatively, though I do not support this option, legislation and regulation could require any website that conditions access on data sharing to offer a more limited alternative that does not require data sharing.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM CHAD A. MARLOW

Q.1. In 2018, pharmaceutical company GlaxoSmithKline announced a partnership with genetic testing kit company 23andMe. The companies touted the move as a step toward future scientific breakthroughs and cures. But critics cautioned that the companies will just use this data for marketing and may put customers' genetic data at risk.

Q.1.a. Should consumers be concerned that pharmaceutical companies have access to their personal genetic data?

A.1.a. Yes. Personal genetic data contains highly sensitive information about the person from whom it was gathered.

Q.1.b. How can we ensure that pharmaceutical companies are using this data for the benefit of society and population health, for example to discover new treatments?

A.1.b. The sharing of genetic data with third parties, such as a pharmaceutical company, should be limited to only that which is essential to complete the transaction or other purpose for which the data was originally provided. Further, where such data is shared by necessity, it should be mandated that the data cannot be used or shared by the third-party recipient for any purpose beyond the essential one for which it was provided, and that it should not be retained any longer than is needed to complete the task for which it was provided, regardless of whether the party in possession of the data is the original recipient of the genetic material/data or a third-party recipient.

Most importantly, even where the use of the genetic data may be for a societally beneficial purpose, a well-designed privacy law must empower people who provide their genetic material to decide what their personally identifiable genetic material, and the data derived therefrom, may and may not be used for. They must also be empowered to demand their genetic material be destroyed, and the data derived therefrom be erased.

Providing a meaningful privacy right with respect to genetic material and the data derived therefrom goes beyond just seeking individual consent to share it. The consent mandated by law must be fully informed, discretely requested and provided, and narrowly tailored, so that the granting of permission to use private genetic material/data for one purpose is not broadly construed to allow many additional uses that have not, in the mind of the person sharing the genetic material, been agreed upon. To that end, for example, requesting permission in the body of a multi-page customer agreement or dense package insert is not sufficient and should be prohibited. Assuming permission has been granted because a consumer did not object ("opt-out permission") is also not adequately protective of privacy. Consumers should have to affirmatively and clearly give specific permission for their genetic material/data to be used for a purpose beyond that for which it was provided ("opt-in permission").

A final point bears making here. The recent disturbing revelation that Google, in a partnership with Ascension, the Nation's second largest health system, has been gathering and sharing the personal health information of tens of millions of patients[1] highlights the problem here. In defense of the program—called "Project Nightingale"—Tariq Shaukat, the President of Industry Products and Solutions for Google Cloud, stated that the goal of the program was to "help healthcare organizations like Ascension improve the healthcare experience and outcomes."[2] Even if this stated goal is accurate, it raises two critical problems. First, whether pursuing a positive societal goal is worth surrendering deeply personal health information is a decision that should be made by individual patients, not by the companies seeking to collect and use their private health information. Federal laws need to be adopted and revised to

[1] *https://www.wired.com/story/google-is-slurping-up-health-dataand-it-looks-totally-legal/*.
[2] *https://cloud.google.com/blog/topics/inside-google-cloud/our-partnership-with-ascension.*

ensure the right of individuals to decide if and how their genetic and other health information is collected and used is clear, unequivocal, and not placed at risk by unintended loopholes. Second, even if the patients' health information is collected by Google for a benevolent public health purpose, there is no certainty that data will not also be used for other purposes that have little or no connection to public health. Federal privacy laws need to be adopted that protect personal privacy through real, enforceable limits on when and under what conditions personal data can be collected, retained, and shared, and a private right of action must be provided to help individuals enforce those rules.

Q.1.c. If Congress were to pass legislation allowing individuals to sell their own data, how should we think about the implications of allowing an individual would to sell their genetic data?

A.1.c. Persons already have the right to sell their personal data, including their genetic data, so Congress does not need to pass legislation to provide that right. Congress should not pass any data-as-property laws that have the effect of encouraging or persuading people to forgo their privacy and sell their data, as doing so would undermine existing and future privacy laws, especially among poorer Americans for whom it is very difficult to say no to additional income, even if the amount promised is uncertain and likely to be small.

Q.1.d. What rights should one individual have to share private health information that describes not only themselves, but also their family members?

A.1.d. While genetic information contains sensitive information about the person providing it, as well as their family members, individuals have the right to share their own personal genetic information.

Q.2. Equifax has repeatedly shown that it is not a proper caretaker for consumer information. In the most recent example, Equifax was found to use the word "admin" as both password and username for a portal that contained sensitive information.

Q.2.a. Do consumers have any recourse against companies like Equifax, companies that repeatedly place sensitive consumer financial information at risk?

A.2.a. While some State data breach and data security laws may provide some consumer recourse rights in this area, there is no broad Federal law that provides such recourse rights to all Americans. In cases where the handling or protection of personal data is negligent, common laws tools may provide recourse. This questions highlights why a comprehensive Federal privacy law should include a robust private right of action.

Q.2.b. How would a property rights in data regime change this situation?

A.2.b. While a strong Federal privacy law could help here, a property rights in data law would, if anything, undermine individual privacy. Passing an unnecessary Federal data-as-property law would have the effect of encouraging people to sell their data, rather than to protect it. That would feed into, rather than reduce, the

risk presented by Equifax-type companies, especially for poorer Americans who will find it more difficult to say no to selling away their private information.

Q.3.a. It is important to recognize that consumer data outlives the relationship with the institution that collects the data.

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.3.a. There are no Federal laws that create universally applicable rules governing consumer data collection, retention, deletion, or security. Each of these constitutes a major gap in privacy protections that urgently need to be addressed in a Federal data privacy law. A strong Federal data privacy law should include a "right of erasure," which is the right of individuals to demand the personal data they furnished to a company be deleted when they terminate their relationship with the company or at any other time upon their request.

Q.3.b. Is there any uniform requirement that mandates institutions treat consumer data a certain way once a consumer decides to no longer conduct business with an institution?

A.3.b. There are no Federal laws that create universally applicable rules governing consumer data retention, deletion, or security once a commercial relationship ends or is terminated. Each of these constitutes a major gap in privacy protections that urgently need to be addressed in a Federal data privacy law.

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

A.3.c. Yes.

Q.3.d. To ensure consumer's 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.3.d. Yes, but Federal law should also give them the option to request their data be deleted.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN FROM CHAD A. MARLOW

Q.1. In your written testimony, you expressed concerns regarding the data-as-property model. Specifically, you mentioned that data-as-property model creates a "hedge" against potential future privacy laws enacted at the State and Federal level. Can you explain further how a data-as-property model could interact with current and potential future privacy laws?

A.1. Presently, with the exception of Federal laws governing financial, health, and children's data, and a few strong State laws, there are very few barriers to prevent private, personal data from flowing from individuals to data collectors to enumerable third parties. This has allowed the marketplace for personal data to flourish at the expense of Americans' personal privacy.

A strong Federal data privacy law, and strong State data privacy laws, would interrupt this flow. Such laws, where adopted, are likely to end the corporate practice of collecting and sharing individual's private, personal information without their knowledge and meaningful consent. To that end, such laws may and should empower individuals to decide what personal data of theirs may be collected and what may be shared. They may and should empower individuals to demand the use of their data be limited to the purpose for which it was collected. They may and should empower individuals to demand their data be deleted after the purpose for which it was collected is completed, or upon a deletion request by the consumer. They may and should empower individuals to make pro-privacy choices without being punished or otherwise disadvantaged compared to those who do not. And they may and should empower individuals to directly sue those who violate their data privacy rights. Not all individuals will take advantage of these privacy protections, but many will. The result will be, in the absence of some countervailing force, that the availability of personal data in the marketplace, and the profits that can be made therefrom, will be reduced.

The data-as-property model is a hedge against stronger privacy laws because it seeks to use the levers of Government power to place that countervailing force directly in front of consumers at the time they would be contemplating exercising their newly bestowed data privacy rights. Specifically, consumers will be reminded of their right to sell their data and, more importantly, of the availability of companies that will facilitate that sale and their receipt of a "royalty payment" for doing so. While the amount individuals will receive for selling their personal information will not be stated, as it will be unknown at the time sales permission is sought, for Americans who are struggling to pay their bills or put food on their tables, the opportunity to earn any extra money—no matter how little and uncertain it may be—may be impossible to refuse.

And so, even if tougher Federal and State privacy laws are passed, the ability to offer people financial incentives to not exercise those new rights will serve as an important hedge again those laws and as an effective way to undermine them, especially when it comes to the most financially needy Americans. These harms are a significant reason why data-as-property bills were rejected by every one of the 11 State legislatures that considered them in 2019.

Q.2. How could a company's incentives change under a data-as-property model with respect to the services they offer consumers?

- Would companies be likely to change their business models in certain circumstances to target consumers of different income levels?
- Would these potential responses conflict with recent State and Federal efforts regarding privacy? If so, how?

A.2. It is difficult to imagine all the ways in which companies might adjust their business models under a data-as-property regime. Could we see startup companies and existing tech giants racing to serve as the "transaction agents" for personal data sales so they can capture the substantial revenues to be made therefrom? Perhaps. Could we see companies paying more money for the

personal data of wealthy individuals compared to poorer individuals because the former would be less likely to consent to selling their data for trivial sums of money? Perhaps. Could we see companies investing huge sums of money in advertising campaigns to encourage individuals to sell their personal information? Perhaps? Could we see a system emerge where corporate data re-sellers and purchasers make huge profits off the sale of personal data, but very little trickles down to the individuals who actually sell their private, personal information? Perhaps.

In the end, the question to ask isn't about if the data-as-property model would conflict with recent Federal and State privacy efforts, but rather if it would undermine them. To that, for the reasons discussed in my answer to your first question, the answer is an unequivocal yes.

Q.3.a. What are the potential tracking requirements that would need to be put in place with a data-as-property model?

A.3.a. The data-as-property model is based on the premise that people should get paid when their data is sold and re-sold. To do that, an elaborate tracking and monitoring system would need to be deployed. That system would have two major components. First, it would require some sort of unique, universal tracking number be attached to all personal data. This is needed to track data as it moves through the virtual world so sellers can ascertain if permission to sell the data has been granted, if any limitations have been placed on its sale, and so the person who originally sold the data can get paid. It is possible that all data will need to be tagged with a tracking number, so potential sellers can determine if sales permission has been granted or denied, and so they know who to request permission from where it has not been granted. The use of these tracking numbers as a unique identifier would have serious negative impacts on data privacy and online anonymity. Second, it would require a comprehensive system of data monitoring to ensure that payments that are due are actually made. Other than proceeding through a weak honor system—because it is easy to copy data and allude tracking—it is hard to imagine how it will be possible to ensure payments are made and how to avoid the development of a black market for commission-free personal data. Undoubtedly, companies that track data and facilitate "royalty" payments will charge fees for their services that may leave little compensation left for those who sell their personal information.

Q.3.b. How would such a model function in the absence of those requirements?

A.3.b. It could not.

Q.4. You have advocated for Congress passing strong privacy laws in lieu of a data-as-property model. What would you consider to be the key elements of a strong privacy law?

A.4. At a minimum, a strong Federal privacy law should:

1) *Place limits on how personal information can be collected, used, and retain*ed. Legislation must include real protections that consider the modern reality of how people's personal information is collected, retained, and used. The law should limit the purposes for which consumer data can be used,

require purging of data after permissible uses have completed, prevent coercive conditioning of services on waiving privacy rights, and limit so called "pay for privacy" schemes. A well-designed Federal privacy law would empower people to choose what degree of privacy they want for themselves. To make this right meaningful, it must go beyond just seeking individual consent. The consent mandated by law must be fully informed, discretely requested and provided, and narrowly tailored, so that the granting of permission to transfer one's data to one third party for a specific purpose is not broadly construed to allow many additional transfers and uses that have not, in the mind of the person sharing the data, been agreed upon. To that end, for example, requesting permission in the body of a multi-page user agreement is not sufficient and should be prohibited. Assuming permission has been granted because a consumer did not object ("opt-out permission") is also not adequately protective of privacy. Consumers should have to affirmatively and clearly give specific permission for their data to be used for any purposes beyond that for which it was provided ("opt-in permission").

2) *Not prevent States from putting in place stronger consumer protections or taking enforcement action.* Any Federal privacy standards should be a floor—not a ceiling—for consumer protections. The ACLU strongly opposes legislation that would, as some industry groups have urged, preempt stronger State laws. Such an approach would put existing consumer protections, many of which are State-led, on the chopping block and prevent additional consumer privacy protections from ever seeing the light of day. We also oppose efforts to limit the ability of State Attorneys General or other regulators from suing, fining, or taking other actions against companies that violate their laws.

3) *Contain strong enforcement mechanisms, including a private right of action.* Federal privacy legislation will mean little without robust enforcement. Thus, any legislation should grant greater resources and enforcement capabilities to the FTC and permit State and local authorities to fully enforce Federal law. To fill the inevitable Government enforcement gaps, however, the ACLU urges Congress to ensure that Federal legislation also grants consumers the right to sue companies for privacy violations.

4) *Guard against discrimination in the digital ecosystem.* Existing Federal laws prohibit discrimination in the credit, employment, and housing context. Any Federal privacy legislation should ensure such prohibitions apply fully in the digital ecosystem and are robustly enforced. In addition, we urge Congress to strengthen existing laws to guard against unfair discrimination, including in cases where it may stem from algorithmic bias.

RESPONSE TO WRITTEN QUESTION OF SENATOR SINEMA FROM CHAD A. MARLOW

Q.1. Opponents of the data-as-property model argue the user is not the sole creator of data and therefore does not deserve sole ownership. This argument is underpinned by the belief that data is a joint-creation of the user and platform because the platform creates an environment and technology to process the data. Most Arizonans are not aware when data brokers collect their data and typically find out when they search their own names and find information about themselves, accurate or otherwise. How would data brokers' practices be treated under a data-as-property model? Would this model provide recourse to Arizonans who wish to address inaccuracies in the personal information data brokers choose to sell?

A.1. To your first question, data-as-property laws would allow consumers to choose to have their data sold to third parties, such as data brokers, or to not have it sold; however, strong Federal data privacy laws could establish this same right without advancing a profit-driven system that influences and encourages persons to sell their data—an approach that would have a particularly deleterious effect on persons with greater financial needs.

A well-designed Federal privacy law would give people control over their information and empower people to choose what degree of privacy they want for themselves. In the scenario presented here, that would mean empowering people to choose whether or not their private information is sold or shared by the original collector with third parties such as data brokers. To make this right meaningful, it must go beyond the broken "inform and consent" model that currently dominates the technology sector. The consent mandated by law must be fully informed, discretely requested and provided, and narrowly tailored, so that the granting of permission to transfer one's data to one third party for a specific purpose is not broadly construed to allow many additional transfers and uses that have not, in the mind of the person sharing the data, been agreed upon. To that end, for example, requesting permission in the body of a multi-page user agreement is not sufficient and should be prohibited. Assuming permission has been granted because a consumer did not object ("opt-out permission") is also not adequately protective of privacy. Consumers should have to affirmatively and clearly give specific permission for their data to be used for any purposes beyond that for which it was provided ("opt-in permission").

To your second question, the data-as-property model contains no right for consumers to request the correction of inaccurate information about them, but such a right could be included in a comprehensive Federal privacy law.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR JONES FROM CHAD A. MARLOW

Discrimination

Q.1. In the Banking Committee, we often discuss discrimination involving loans and housing. As technology helps companies become more sophisticated it is easier to put in place discriminatory

policies. Are there are protections currently in place that prevent data discrimination by race, gender, or religion? If not, what methods should Congress consider to decrease discrimination within data?

A.1. Existing Federal laws prohibit discrimination in the credit, employment, and housing context. However, our existing infrastructure is insufficient to safeguard against discrimination in the digital world for several reasons.

First, many online providers have been slow to fully comply with Federal antidiscrimination laws—and in many cases plaintiffs face challenges in getting the information necessary to raise discrimination claims. For example, Facebook recently settled a lawsuit brought by ACLU and other civil rights organizations amid allegations that it discriminated on the basis of gender and age in targeting ads for housing and employment.[1] The lawsuit followed repeated failures by the company to fully respond to studies demonstrating that the platform improperly permitted ad targeting based on prohibited characteristics, like race, or proxies for such characteristics. The company is also now the subject of charges brought by the Department of Housing and Urban Development (HUD), which includes similar allegations.[2]

Second, there have been efforts to weaken existing laws in ways that would make it more difficult to address algorithmic discrimination. For example, HUD recently proposed amending the existing Disparate Impact Rule, codified at 24 C.F.R. § 100.500, to make it more difficult for plaintiffs to raise discrimination claims based on disparate impact. Among other things, the Proposed Rule would allow a defendant to avoid liability for using an algorithmic model that disproportionately excludes members of protected classes if the defendant can prove one of three defenses, any of which will operate as a complete defense, with no opportunity for a plaintiff to prove the existence of less discriminatory alternatives to achieve any legitimate business objectives.

Third, our existing laws need to be expanded to address digital discrimination that occurs outside the housing, credit, and employment context. For example, commercial advertisers should not be permitted to offer different prices, services, or opportunities to individuals, or to exclude them from receiving ads offering certain commercial benefits, based on characteristics like their gender or race. And regulators and consumers should be given information and tools to address algorithms or machine learning models that disparately impact individuals on the basis of protected characteristics.

Federal law must be strengthened to address these challenges. First, Federal privacy law should make clear that existing antidiscrimination laws apply fully in the online ecosystem, including in online marketing and advertising. Federal agencies that enforce these laws, like HUD, the EEOC, and the Consumer Financial Protection Bureau, should be fully resourced and given the technical

---

[1] ACLU, *Facebook Agrees to Sweeping Reforms to Curb Discriminatory Ad Targeting Practices* (Mar. 19, 2019), *https://www.aclu.org/news/facebook-agrees-sweeping-reforms-curb-discriminatory-ad-targeting-practices.*

[2] Complaint of Discrimination Against Facebook, FHEO No. 01–18–032308, *https://www.hud.gov/sites/dfiles/Main/documents/HUD__v__Facebook.pdf.*

capabilities to vigorously enforce the law in the context of these new forms of digital discrimination. In addition, companies should be required to audit their data processing practices for bias and privacy risks, and such audits should be made available to regulators and disclosed publicly, with redactions if necessary to protect proprietary information. Finally, researchers should be permitted to independently audit platforms for bias, and Congress should not permit enforcement of terms of service that interfere with such testing.

Data Privacy

Q.2.a. So much of data privacy is having the choice to share information. For example, many people find targeted ads to be disturbing and others find it serves as a helpful reminder. How should policymakers consider different preferences as they write legislation on personal data privacy and how it is used?

A.2.a. Privacy is not a condition to be imposed upon individuals, but a right to be meaningfully provided. That means a well-designed privacy law would empower people to choose what degree of privacy they want for themselves. In the scenario presented here, that would mean empowering people to choose if they want to allow their personal data to be collected and used to provide them with targeted ads or if they do not.

But providing a meaningful right goes beyond just seeking individual consent. The consent mandated by law must be fully informed, discretely requested and provided, and narrowly tailored, so that the granting of permission to use private information for one purpose is not broadly construed to allow many additional uses that have not, in the mind of the person sharing the data, been agreed upon. To that end, for example, requesting permission in the body of a multi-page user agreement is not sufficient and should be prohibited. Assuming permission has been granted because a consumer did not object ("opt-out permission") is also not adequately protective of privacy. Consumers should have to affirmatively and clearly give specific permission for their data to be used for any purposes beyond that for which it was provided ("opt-in permission").

In addition, the law should be made unambiguously clear that the data cannot be used to discriminate against users. At a minimum, with respect to targeted advertising, discriminatory practices that are prohibited in the physical world should be equally prohibited on the internet.

Q.2.b. Many services require information from one site to be shared to another in order for the consumer to have access to the website's services. Sometimes this information sharing is helpful and makes the website more user friendly but sometimes the data shared does not have any obvious benefits to the consumer.

A.2.b. The vast majority of data sharing among web sites takes place for the purpose of advertiser-driven consumer tracking—something polls find Americans remain deeply uncomfortable with but feel helpless to stop. Where the sharing of data with third parties is genuinely necessary for providing a service consumers find useful, such sharing should be limited only to data that is essential

to complete the transaction or other purpose for which it was originally provided. Further, where such data is shared by necessity with a third party, it should be mandated that the data cannot be used or re-shared by the third-party recipient for any purpose beyond the essential one for which it was provided. Beyond that, should Federal law put strong opt-in privacy protections in place, data should be sharable beyond the purpose for which it was originally provided if—and only if—the user-provider has given clear, well-informed, and discrete opt-in consent.

Q.3. I am concerned that Congress will enact data privacy legislation but then websites will deny access to consumers for simply not approving sharing their data. Should consumers be denied access for not approving data sharing?

A.3. This is an important concern. Privacy rights will be of little value if individuals who choose to exercise them can be punished or denied benefits for doing so. Federal law should protect those who elect to exercise their privacy rights by prohibiting companies from denying service, providing worse service, or charging higher prices to those who exercise their privacy rights, as well as prohibiting them from providing better service, lower prices, or other benefits to those who do not exercise their privacy rights.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN FROM WILL RINEHART

Q.1. In your written testimony, you mentioned that creating a property right for data could make it more difficult for consumers to control their data. Can you provide further detail regarding how a data-as-property model could interact with privacy protections in current laws, such as the Fair Credit Reporting Act?

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

Q.2. Your written testimony also discusses the different methodologies to value data.

- How could information asymmetry between companies and consumers impact the valuation of data under the different methods you described?
- Under any of the models you mentioned, do you believe that customers will have the ability to determine the value of their data before a given transaction?

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

Q.3. How could a company's incentives change under a data-as-property model with respect to the services they offer consumers?

- Would companies be likely to change their business models in certain circumstances to target consumers of different income levels?
- Would these potential responses conflict with recent State and Federal efforts regarding privacy? If so, how?

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

RESPONSES TO WRITTEN QUESTIONS OF SENATOR JONES FROM WILL RINEHART

Discrimination

Q.1. In the Banking Committee, we often discuss discrimination involving loans and housing. As technology helps companies become more sophisticated it is easier to put in place discriminatory policies. Are there are protections currently in place that prevent data discrimination by race, gender, or religion? If not, what methods should Congress consider to decrease discrimination within data?

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

Data Privacy

Q.2. So much of data privacy is having the choice to share information. For example, many people find targeted ads to be disturbing and others find it serves as a helpful reminder. How should policymakers consider different preferences as they write legislation on personal data privacy and how it is used?

Many services require information from one site to be shared to another in order for the consumer to have access to the website's services. Sometimes this information sharing is helpful and makes the website more user friendly but sometimes the data shared does not have any obvious benefits to the consumer.

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

Q.3. I am concerned that Congress will enact data privacy legislation but then websites will deny access to consumers for simply not approving sharing their data. Should consumers be denied access for not approving data sharing?

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

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM MICHELLE DENNEDY

Q.1. It is important to recognize that consumer data outlives the relationship with the institution that collects the data.

Q.1.a. 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?

Q.1.b. Is there any uniform requirement that mandates institutions treat consumer data a certain way once a consumer decides to no longer conduct business with an institution?

Q.1.c. If the data collecting company is breached after the consumer has terminated their relationship, is the consumer's data still vulnerable?

Q.1.d. To ensure consumer's 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.1.a.–d. Response not received in time for publication.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR JONES FROM MICHELLE DENNEDY

Discrimination

Q.1. In the Banking Committee, we often discuss discrimination involving loans and housing. As technology helps companies become more sophisticated it is easier to put in place discriminatory policies. Are there are protections currently in place that prevent data discrimination by race, gender, or religion? If not, what methods should Congress consider to decrease discrimination within data?

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

Data Privacy

Q.2. So much of data privacy is having the choice to share information. For example, many people find targeted ads to be disturbing and others find it serves as a helpful reminder. How should policy makers consider different preferences as they write legislation on personal data privacy and how it is used?

Many services require information from one site to be shared to another in order for the consumer to have access to the website's services. Sometimes this information sharing is helpful and makes the website more user friendly but sometimes the data shared does not have any obvious benefits to the consumer.

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

Q.3. I am concerned that Congress will enact data privacy legislation but then websites will deny access to consumers for simply not approving sharing their data. Should consumers be denied access for not approving data sharing?

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

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

October 23, 2019

The Honorable Mike Crapo, Chairman
The Honorable Sherrod Brown, Ranking Member
U.S. Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

We write to you regarding your hearing on "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation."[1] EPIC appreciates your attention to privacy, but believes this hearing's focus on ownership is misguided. An approach based on data ownership and portability will accelerate industry consolidation. It ducks the hard the problem of breaking up big tech, helps not all with data protection, and imagines markets that do not exist.

EPIC is a public-interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is a leading advocate for consumer privacy and has appeared before this Committee on several occasions.[3]

Data portability will make it easier for companies such as Facebook to ingest the personal data of the of the firms it acquires. Data portability does not help consumers, but it facilitates mergers and consolidation.

Facebook's acquisition of WhatsApp is a case study of the consumer harm caused by data portability. Facebook now intends to integrate the personal data of WhatsApp users into Facebook, in violation of the representations that Facebook and WhatsApp made to the FTC in 2014.

In 2014, Facebook purchased WhatsApp, a text-messaging service that attracted users specifically because of strong commitments to privacy.[4] WhatsApp's founder stated in 2012 that,

---

[1] *Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation*, 116th Cong. (2019), S. Comm. on Banking, Housing, and Urban Affairs (Oct. 24, 2019), https://www.banking.senate.gov/hearings/data-ownership-exploring-implications-for-data-privacy-rights-and-data-valuation.
[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] *See, e.g, Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing Before the House Comm. on Financial Services, Subcomm. on Financial Institutions and Consumer Credit*, 115th Cong. (2018) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/testimony/congress/EPIC-Testimony-HFS-2-14-18.pdf; *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the House Comm. on Financial Services, Subcomm. Financial Institutions and Consumer Credit*, 112th Cong. (2011) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf.
[4] EPIC, *In re: WhatsApp*, https://epic.org/privacy/internet/ftc/whatsapp/.

"[w]e have not, we do not and we will not ever sell your personal information to anyone."[5] EPIC and the Center for Digital Democracy urged the Federal Trade Commission to block the deal.[6] As we explained at the time:

> WhatsApp built a user base based on its commitment not to collect user data for advertising revenue. Acting in reliance on WhatsApp representations, internet users provided detailed personal information to the company including private text to close friends. Facebook routinely makes use of user information for advertising purposes and has made clear that it intends to incorporate the data of WhatsApp users into the user profiling business model. The proposed acquisition will therefore violate WhatsApp users' understanding of their exposure to online advertising and constitutes an unfair and deceptive trade practice, subject to investigation by the Federal Trade Commission.[7]

The FTC ultimately approved the merger after Facebook and WhatsApp promised not to make any changes to WhatsApp users' privacy settings.[8] However Facebook announced in 2016 that it would begin acquiring the personal information of WhatsApp users, including phone numbers, directly contradicting their previous promises to honor user privacy.[9] Following this, EPIC and CDD filed another complaint with the FTC in 2016, but the Commission has taken no further action.[10] Notably, the recent FTC order with Facebook does not include any restrictions related to WhatsApp.[11]

Meanwhile, European regulators have recognized the problem of Facebook integrating WhatsApp user data. In 2017, the European Commission fined Facebook €110 million for making misrepresentations during the Commission's investigation of the WhatsApp acquisition.[12] Facebook told the Commission it was unable to match WhatsApp user accounts with Facebook user accounts, when the company was aware that it had the technical capability to do so.[13] Germany's competition

---

[5] WhatsApp, *Why We Don't Sell Ads* (June 18, 2012), https://blog.whatsapp.com/245/Why-we-dont-sell-ads.
[6] EPIC and Center for Digital Democracy, Complaint, Request for Investigation, Injunction, and Other Relief In the Matter of WhatsApp, Inc., (Mar. 6, 2014), https://epic.org/privacy/ftc/whatsapp/WhatsApp-Complaint.pdf.
[7] *Id.* at 1.
[8] *See*, Letter from Jessica L. Rich, Dir., Bureau of Consumer Prot., Fed. Trade Comm'n, to Facebook and WhatsApp (Apr. 10, 2014), https://epic.org/privacy/internet/ftc/whatsapp/FTC-facebook-whatsapp-ltr.pdf (concerning the companies' pledge to honor WhatsApp's privacy promises).
[9] WhatsApp, *Looking Ahead for WhatsApp* (Aug. 25, 2016), https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp.
[10] EPIC and Center for Digital Democracy, Complaint, Request for Investigation, Injunction, and Other Relief In the Matter of WhatsApp, Inc. (Aug. 29, 2016), https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf; Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation*, Techonomy (May 4, 2018), https://techonomy.com/2018/05/facebook-whatsapp-lesson-privacy-protection-necessary-innovation.
[11] Decision and Order, *In re Facebook, Inc.*, FTC File No. 1823109 (July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.
[12] European Commission, *Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover* (May 18, 2017), https://europa.eu/rapid/press-release_IP-17-1369_en.htm.
[13]

agency has imposed restrictions on Facebook's practice of combining user data from across its platforms, such as WhatsApp and Instagram, and prohibited the company from linking third-party data to specific Facebook user accounts.[14]

Facebook now intends to integrate WhatsApp, Instagram, and Facebook Messenger.[15] U.S. regulators are not responding to this threat to privacy and competition. Data portability would make this process easier for giants like Facebook, facilitating further consolidation in the technology sector.

A Better Approach to Privacy

Baseline federal legislation should be built on a familiar privacy framework, such as the original U.S. Code of Fair Information Practices and the widely followed OECD Privacy Guidelines. The rights and responsibilities set out in these frameworks are necessarily asymmetric: the individuals that give up their personal data to others get the rights; the companies that collect the information take on the responsibilities. This is the approach that the United States, the European Union, and others have always taken to establish and update privacy laws concerning the collection and use of personal data.

EPIC recently released *Grading on a Curve: Privacy Legislation in the 116th Congress.* EPIC's report set out the key elements of a privacy law. As it considers comprehensive data privacy legislation, Congress should include:

Strong definition of personal data

The scope of a privacy bill is largely determined by the definition of personally identifiable information or "personal data," in the terminology of the GDPR. A good definition recognizes that personal data includes both data that is explicitly associated with a particular individual and also data from which it is possible to infer the identity of a particular individual. A good definition of personal data will typically include a non-exclusive list of examples. Personal data also includes all information about an individual, including information that may be publicly available, such as zip code, age, gender, and race. All of these data elements are part of the profiles companies create and provide the basis for decision-making about the individual. So, bills that exclude publicly available information misunderstand the purpose of a privacy law.

Establishment of an Independent Data Protection Agency

Almost every democratic country in the world has an independent federal data protection agency, with the competence, authority, and resources to help ensure the protection of personal data. These agencies act as an ombudsman for the public. The United States has tried for many years to create agencies that mimic a privacy agency, such as the Privacy and Civil Liberties Oversight

---

[14] *Bundeskartellamt prohibits Facebook from combining user data from different sources* (July 2, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[15] Mike Isaac, *Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger*, N.Y. Times (Jan. 25, 2019), https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html.

Board, or to place responsibilities at the Federal Trade Commission. Many now believe that the failure to establish a data protection agency in the United States has contributed to the growing incidents of data breach and identity theft. There is also reason to believe that the absence of a U.S. data protection agency could lead to the suspension of transborder data flows following recent decisions of the Court of Justice of the European Union.[16]

Individual rights (right to access, control, delete)

The purpose of privacy legislation is to give individuals meaningful control over their personal information held by others. This is accomplished by the creation of legal rights that individuals exercise against companies that choose to collect and use their personal data. These rights typically include the right to access and correct data, to limit its use, to ensure it is security protected, and also that it is deleted when no longer needed. "Notice and consent," although it appears in several of the proposed bills, has little to do with privacy protection. This mechanism allows companies to diminish the rights of consumers, and use personal data for purposes to benefit the company but not the individual.

Strong data controller obligations

Organizations that choose to collect and use personal data necessarily take on obligations for the collection and use of the data. These obligations help ensure fairness, accountability, and transparency in decisions about individuals. Together with the rights of individuals describes above, they are often described as "Fair Information Practices." Many of these obligations are found today in U.S. sectoral laws, national laws, and international conventions. These obligations include:

- Transparency about business practices
- Data collection limitations
- Use/Disclosure limitations
- Data minimization and deletion
- Purpose specification
- Accountability
- Data accuracy
- Confidentiality/security

Require Algorithmic Transparency

As automated decision-making has become more widespread, there is growing concern about the fairness, accountability, and transparency of algorithms. All individuals should have the right to know the basis of an automated decision that concerns them. Modern day privacy legislation typically includes provisions for the transparency of algorithms to help promote auditing and accountability. For example both the GDPR and the Council of Europe Privacy Convention—new laws that address emerging privacy challenges—have specific articles to ensure accountability for algorithmic-based decision-making.

[16] EPIC, *Max Schrems v. Data Protection Commissioner (CJEU - "Safe Harbor")*, https://epic.org/privacy/intl/schrems/.

Require Data Minimization and Privacy Innovation

Many U.S. privacy laws have provisions intended to minimize or eliminate the collection of personal data. Data minimization requirements reduce the risks to both consumers and businesses that could result from a data breach or cyber-attack.

Good privacy legislation should also promote privacy innovation, encouraging companies to adopt practices that provide useful services and minimize privacy risk. Privacy Enhancing Techniques ("PETs") seek to minimize the collection and use of personal data.

Prohibit take-it-or-leave-it or pay-for-privacy terms

Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.

Private Right of Action

Privacy laws in the United States typically make clear the consequences of violating a privacy law. Statutory damages, sometimes called "liquidated" or "stipulated" damages are a key element of US privacy law and should provide a direct benefit to those whose privacy rights are violated. Several of the bills pending in Congress rely on the Federal Trade Commission to enforce privacy rights, but the FTC is ineffective. The agency ignores most complaints it receives, does not impose fines on companies that violate privacy, and is unwilling to impose meaningful penalties on repeat offenders.[17]

Limit Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government would be able to collect personal data in bulk from companies, a form of "mass surveillance" enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.[18]

Do Not Preempt Stronger State Laws

A well-established principle in the United States is that federal privacy law should operate as a floor and not a celling. That means that Congress often passes privacy legislation that sets a minimum standard, or "baseline," for the country and allows individual states to develop new and innovative approaches to privacy protection. The consequences of federal preemption are potentially severe and could include both a reduction in privacy protection for many consumers, particularly in California, and also a prohibition on state legislatures addressing new challenges as they emerge.

---

[17] Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.*, FTC File No. 1823109 at 17 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

[18] *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

That could leave consumers and businesses exposed to increasing levels of data breach and identity theft from criminal hackers and foreign adversaries.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

Christine Bannan
Christine Bannan
EPIC Consumer Protection Counsel

Enclosures:
EPIC, *Grading on a Curve: Privacy Legislation in the 116th Congress* (2019)

October 23, 2019

The Honorable Mike Crapo
Chairman
The U.S. Senate Banking, Housing, and
Urban Affairs Committee
U.S. Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
The U.S. Senate Banking, Housing, and
Urban Affairs Committee
U.S. Senate
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of ACA International, I am writing in regard to your hearing entitled, "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation." ACA International is the leading trade association for credit and collection professionals representing approximately 3,000 members, including credit grantors, third-party collection agencies, asset buyers, attorneys, and vendor affiliates in an industry that employs more than 230,000 employees worldwide.

Without an effective collection process, the economic viability of businesses and, by extension, the American economy in general, is threatened. Recovering rightfully-owed consumer debt enables organizations to survive, helps prevent job losses, keeps credit, goods, and services available, and reduces the need for tax increases to cover governmental budget shortfalls. Furthermore, without the information that ACA members provide to consumers, they cannot make informed decisions that help preserve their ability to access credit, medical care, and a host of other goods and services. ACA members play a key role in helping consumers fulfill

Almost half (44 percent) of ACA member organizations (831 companies) have fewer than nine employees. Furthermore, 85% of members (1,624 companies) have 49 or fewer employees and 93% of members (1,784 companies) have 99 or fewer employees. Overall, 87 percent of ACA members are small businesses. As such, we appreciate that the Senate Banking Committee is considering implications for data privacy.

We strongly support the goal of protecting the privacy of consumers and their data, and are committed to vigorous compliance in furtherance of this pursuit. However, there are many lawful and important reasons why those in the accounts receivables management industry may collect and store consumer data in compliance with already existing privacy and consumer protection laws. As Congress moves forward, it is critical that it is diligent in ensuring legitimate businesses are not faced with insurmountable regulatory burdens surrounding data privacy laws, particularly if they stifle innovation or have a disproportional impact on small businesses.

ASSOCIATION HEADQUARTERS
4040 WEST 70TH STREET 55435
P.O. BOX 390106, MINNEAPOLIS, MN 55439-0106
TEL (952) 926-6547 FAX (952) 926-1624

FEDERAL GOVERNMENT AFFAIRS OFFICE
509 2ND STREET NE, WASHINGTON, D.C. 20002
TEL (202) 547-2670
FAX (202) 547-2671

ACA@ACAINTERNATIONAL.ORG WWW.ACAINTERNATIONAL.ORG

The current landscape for compliance in this area for the industry is robust including sweeping and complex state legislation such as the California Consumer Privacy Act of 2018 (CCPA), which also touches many businesses outside of California. Additionally, there are multiple federal laws ACA members are already complying with in this area including the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act (FDCPA), the Gramm Leach Bliley Act, and the Family Educational Rights and Privacy Act of 1974. Notably, the industry is already very restricted in what information and how information can be communicated to consumers under the FDCPA, and Congress should carefully consider these requirements in consultation with the Consumer Financial Protection Bureau as it crafts any new legislation in this area. Furthermore, the General Data Protection Regulation went into effect in the European Union in May 2018 and impacts certain ACA members in the United States, as well as international accounts receivable management agencies.

As Congress moves forward with any potential new laws for federal data privacy, we ask that it is cautious not to create any duplicative, conflicting, or overly complex standards for those in the accounts receivable management industry who already work carefully to protect consumer data. ACA and its members have also outlined their concerns specific to the CCPA in hearings and through comments at the state level. We ask that you consider that feedback and those concerns if the Committee looks to different state laws, as it considers a federal standard.

Lastly, we strongly urge Congress that any law going forward should preempt state requirements, so that all Americans receive the same level of privacy protections. Thank you for holding this important hearing. We look forward to continuing our engagement with the Senate Banking Committee and other Congressional committees exploring this issue.

Sincerely,

Mark Neeb
Chief Executive Officer

October 24, 2019

United States Senate
Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

Re: October 24, 2019 Full Committee Hearing on Data Ownership: Exploring Implications for Data Privacy Rights and Data Evaluation

Dear Chairman Crapo and Ranking Member Brown:

Consumer Reports[1] writes to urge the US Senate Committee on Banking, Housing, and Urban Affairs to reject policy proposals based on quasi-property rights over data, or that respond to consumers' concern around data selling by simply giving them a cut of the action. For over 80 years, we have worked with consumers for truth, transparency, and fairness in the marketplace. And, we are strong proponents of legislation that bolsters consumers' privacy and their individual right to choose who accesses their data and for what purposes. It is within this framework that we must recommend that the Committee reject the false solution of data ownership and the dangerous precedent it establishes. Furthermore, privacy is an inalienable human right that cannot be traded away, even if a monetary value of a consumer's data could be assessed.

We appreciate your interest in protecting individual privacy in the United States and ensuring fairness in the marketplace, but advancing data ownership as a possible solution does neither. It would instead risk turning the basic right to privacy into a luxury out of reach to lower-income Americans. Indeed, consumers desire more control over their private information and dislike such information being shared and monetized in this way.[2]

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For 83 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] For example, a Consumer Reports survey found that 92 percent of Americans think companies should get permission before sharing or selling users' online data and that 70 percent of Americans lack confidence that their personal information is private and secure. *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017),

For this reason, we have strenuously advocated against pay-for-privacy regimes in which companies give consumers a discount on services in exchange for gaining access to, and the ability to monetize, a consumer's personal data.[3] In response to consumer outcry, many of these types of proposals have been abandoned. For instance, in 2016 AT&T offered a pay-for-privacy plan with poor results.[4] Not only was it confusing and difficult for consumers to opt out of the collection and use of their data in the first place, the disparity between the privacy protective plan and the discounted plan was $30 dollars a month, a significant portion of the monthly charge for internet service. This discounted amount was not tied to the relative value of the personal data being shared: "The inducement engendered by such a steep discount, which did not even appear tied to the monetary value of the data, effectively took away the ability of AT&T customer to make a reasoned choice about their privacy."[5] In addition, it is hard to conceive of a workable model in which consumers could claim property rights over their information since data is often co-created, useful only when combined with other data, and, unlike physical goods, can be held by many at once and easily disseminated. All of these issues present serious obstacles to applying traditional ownership rights over personal data.[6]

---

https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/. In addition, 88 percent of individuals say it is important that they not have someone watch or listen to them without their permission. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. A Mozilla study found that a third of people feel like they have no control of their information online. *Hackers, Trackers, and Snoops: Our Privacy Survey Results*, MOZILLA (Mar. 9, 2017), https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5. The majority of consumers (74%) find it is "very important" to be in control of who can get information about them. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. Indeed, this is not a new sentiment for consumers: a Pew research poll in 2014 found that 91% of adults ""agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies." (Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.)

[3] *See State Broadband Privacy Issue Brief*, CONSUMER REPORTS (Aug. 27, 2019), https://advocacy.consumerreports.org/research/state-broadband-privacy/.

[4] *See* Karl Bode, *AT&T's $30 'Don't Be Snooped On' Fee is Even Worse than Everybody Thought*, TECHDIRT (Mar. 2, 2015), https://www.techdirt.com/articles/20150219/11473630072/ats-30-dont-be-snooped-fee-is-even-worse-than-everybody-thought.shtml. Comcast has discussed offering a similar program in regulatory filings. *See Comments to the Fed. Commc'n Comm'n Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106*, COMCAST (Aug. 1, 2016), https://assets.documentcloud.org/documents/3004210/Comcast-FCC-Filing.pdf.

[5] *Open Technology Institute Publishes Model State Legislation for Broadband Privacy*, OPEN TECH. INST. (Oct. 30, 2017), https://www.newamerica.org/oti/press-releases/open-technology-institute-publishes-model-state-legislation-broadband-privacy/.

[6] Dylan Gilbert, *Federal Privacy Legislation Should Not Be Based on Data Ownership*, PUB. KNOWLEDGE (June 27, 2019), https://www.publicknowledge.org/blog/federal-privacy-legislation-should-not-be-based-on-data-ownership/.

In formalizing the market for the sale of personal information, legislation advancing data ownership would coerce consumers to sign away their right to privacy, without the full context to understand the impact a single sale could have for themselves and our broader society. Furthermore, individuals who sell their data would receive compensation for something that cannot realistically be appraised, or its loss fully reimbursed.[3] Instead, privacy should be understood as an inalienable human right that cannot be bought or sold.

For these reasons, we urge the Committee to focus on legislative proposals that give consumers substantive rights over data, in addition to requiring companies to minimize the amount of data collected about consumers in the first case.

Designing privacy rights around the basic human right to privacy

As technology evolves, consumer trust in the continued existence of genuine privacy is eroding. Yet, although trust is decaying, that troublesome future is not inevitable. But, this bill could hasten its arrival.

There is already an opaque market for consumers' personal information and consumers are left out of the profit chain. But the solution is not to pay Americans to give up their privacy—they deserve privacy rights to shield their personal information from being monitored and sold by data brokers. It would also lend credibility to a market that has been truly harmful for consumers. One that enabled the collection and use of data to create psychological profiles of voters for illicit political purposes[4]; and that enables businesses to create alternative, non-evidence based and potentially discriminatory, credit scores based on consumers' digital footprint.[5]

---

[3] "Figuring out precisely what value consumers place on their personal data is starting to look like a fool's errand...That's partly because the dollar amounts people attach to data privacy in various studies are all over the map. In Winegar and Sunstein's survey, the $5 per month and $80 per month figures are medians. But a fraction of respondents valued their privacy at wildly higher levels — in the hundreds or even thousands per month — while 14% were willing to hand over all their data to internet companies for free.
While the variation tends to be less extreme in experiments involving actual money, it makes sense that people would value online privacy very differently." Will Oremus, *How Much Is Your Privacy Really Worth?*, ONEZERO (Sept. 17, 2019), https://onezero.medium.com/how-much-is-your-privacy-really-worth-421796dd9220.

[4] Ahead of the 2016 presidential election, Cambridge Analytica acquired data on Facebook users through an online entertainment quiz, which was only completed by about 270,000 people but revealed data on 50 million individuals. This was a prominent example of how data collected through seemingly innocuous ways can be used for illicit purposes. Jerry Beilinson, *Facebook Data May Have Been Illicitly Used for Politics, and It Started with a Quiz*, CONSUMER REPORTS (March 17, 2018), https://www.consumerreports.org/privacy/facebook-data-illicitly-collected-for-politics-and-what-it-means-for-privacy/.

[5] *Working Paper: On the Rise of FinTechs – Credit Scoring Using Digital Footprints*, NAT'L BUREAU OF ECON. RESEARCH (April 2018, Revised July 2018), https://www.fdic.gov/bank/analytical/cfr/2018/wp2018/cfr-wp2018-04.pdf. This study raises the concern that the digital footprint may be used as a proxy for legally prohibited variables—such as race, color, gender, national origin, and religion, which can lead to discrimination.

We thank you for recognizing the need to get privacy rights back on track, and for your willingness to approach the fraught issue of consent in the developing data economy. Rather than moving this flawed data ownership concept forward, we urge you to put forward legislation that focuses on shoring up individual privacy as a basic human right.

Legislation that encourages data minimization, gives people agency over the sale and sharing of data, guaranteed transparency into what companies do with that information, and the right to take companies to court for violating those rights, is what Americans need to ensure that privacy continues to be a human right now and in the future.

We stand at a critical juncture for individual privacy rights. Now is the time for the U.S. Congress to pass privacy legislation that prioritizes Americans, not legislation that fortifies a status quo that is eroding fairness and trust in the marketplace.

Sincerely,

Katie McInnis
Policy Counsel

Consumer Reports
1101 17th Street NW
Suite 500
Washington, DC 20036

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

October 23, 2019

The Honorable Michael Crapo
Chairman
Committee on Banking, Housing,
& Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing,
& Urban Affairs
United States Senate
Washington, DC 20510

Re: Today's Hearing: "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation"

Dear Chairman Crapo and Ranking Member Brown:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in conjunction with tomorrow's hearing, entitled "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 118 million consumers with personal and small business financial service products. NAFCU and our members welcome the Committee taking this next step in examining consumer privacy and data security standards by holding this hearing.

As NAFCU wrote to the Committee on June 11, 2019, we believe there is an urgent need for a national data security standard for those who collect and store consumer information. While depository institutions have had a national standard on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA) over two decades ago, other entities who handle consumer financial data do not have such a national standard. Along those same lines, we also believe that there is a need for a uniform national consumer data privacy standard as opposed to a patchwork of standards stemming from different state data privacy laws. Such a standard should recognize what has been in place and is working for consumers, credit unions and others under existing laws such as the GLBA. We hope today's hearing can be another step toward achieving these goals.

NAFCU looks forward to working with the Committee and those in industry to address these concerns with consumer privacy and data security. We would urge you to work collaboratively with other interested Committees in the Senate to find a package that can advance and receive bipartisan support.

On behalf of our nation's credit unions and their more than 118 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information, please contact me or Janelle Relfe, NAFCU's Associate Director of Legislative Affairs, at 703-842-2237 or jrelfe@nafcu.org.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Senate Banking Committee