This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

Diversified Reporting Services, Inc.

RPTS CARR

HIF109020

WHO IS SELLING YOUR DATA: A CRITICAL EXAMINATION OF THE ROLE OF DATA BROKERS IN THE DIGITAL ECONOMY

Wednesday, April 19, 2023

House of Representatives,

Subcommittee on Oversight and Investigations,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 2:00 p.m., in Room 2322, Rayburn House Office Building, Hon. Morgan Griffith [chairman of the subcommittee] presiding.

Present: Representatives Griffith, Burgess, Guthrie, Duncan, Palmer, Lesko, Armstrong, Cammack, Rodgers (ex

officio); Castor, DeGette, Schakowsky, Tonko, Ruiz, Peters, and Pallone (ex officio).

Also present: Representative Trahan.

Staff Present: Sean Brebbia, Chief Counsel; Deep Buddharaju, Senior Counsel; Sarah Burke, Deputy Staff Director; Lauren Eriksen, Clerk; Tara Hupman, Chief Counsel; Sean Kelly, Press Secretary; Peter Kielty, General Counsel; Emily King, Member Services Director; Chris Krepich, Press Secretary; John Strom, Counsel; Michael Taggart, Policy Director; Joanne Thomas, Counsel; Austin Flack, Minority Junior Professional Staff Member; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; Lisa Hone, Minority Chief Counsel, Innovation, Data, and Commerce; Liz Johns, Minority GAO Detailee; Will McAuliffe, Minority Chief Counsel, Oversight and Investigations; Christina Parisi, Minority Professional Staff Member; Harry Samuels, Minority Oversight Counsel; Caroline Wood, Minority Research Analyst; and C.J. Young, Minority Deputy Communications Director.

*Mr. Griffith. The Subcommittee on Oversight and Investigations will now come to order.

The chair now recognizes himself -- that would be me -- for five minutes for an opening statement.

Welcome, everyone, to what I hope will be a productive fact-finding hearing on the current state of the data broker ecosystem.

It is obvious from the testimony that a staggering amount of information is collected on Americans every day, frequently without their knowledge or consent. This data then gets shared, analyzed, combined with other data sets, bought, and sold. In some cases, this data is not even anonymized, meaning that it is easy for bad actors to find deeply personal information on individuals such as their location, demographic data, health information. Some of these data brokers are companies that most people are familiar with, but others operate in the shadows, with many Americans never knowing that they have collected -- that their data has been collected, bought, or sold.

The Federal Trade Commission recently fined an online mental health company, BetterHelp, 7.8 million for disclosing

patients' personal health information to advertising platforms such as Facebook and Google without the users' consent.

Siphoning off private data of Americans on mobile apps is so incredibly easy. All a data broker has to do is pay an app developer a nominal fee to implant a program within the app that is designed to capture the data of all users. Companies rely on these convoluted and unclear terms of service and privacy policy documents, knowing full well users will find it far too tedious to read them before unwittingly agreeing to have their sensitive data accessed by third-party strangers.

There is a complete lack of safeguards surrounding this data, and I am particularly concerned with the implications that has on the sick, the elderly, the youth, and the military. Recent research from Duke University has found data brokers without any accountability can freely collect and share Americans' private mental health data.

We have all heard about the national security concerns raised about the Chinese Communist Party-influenced ByteDance, the parent company of TikTok video app, operating

in our country and collecting data on Americans, while also having the ability to potentially manipulate American public opinion on any given subject matter.

While the current state of play is -- the current state of play in the data broker industry presents some of these same concerns, according to what we will hear today from these, our invited experts, data brokers gather package and advertise highly sensitive data on current and former members of the U.S. military, posing privacy and safety risks to all service members. This, in and of itself, could be considered a security risk if the data collected is identifiable. By collecting and selling data at will, these companies put all Americans at risk.

I look forward to learning from our witnesses today more about how data brokers are collecting, packaging, and analyzing data on Americans, and possible safeguards that we should explore.

[The prepared statement of Mr. Griffith follows:]

**********COMMITTEE INSERT**********

*Mr. Griffith. And with that I yield back, and now recognize the ranking member of the subcommittee, Ms. Castor, for her opening statement.

*Ms. Castor. Well, thank you, Mr. Chairman, for calling this hearing. Thank you to our expert witnesses for being with us today to share your insight on the excesses of the data broker industry. I am grateful that we can take on these issues in a true bipartisan fashion.

These incessant surveillance and data gathering for profit by data brokers affects every American. Data brokers are often invisible to consumers. They rarely interact directly with us, but they are constantly collecting our personal private information, including names, geolocation data, addresses, health data, age, political preferences, and much more. And they collect it no matter how private and sensitive that data may be.

I believe each and every American should determine what personal information to share with a corporation, and then not be held over a barrel if they choose not to do so, especially with the track record now of data breaches and scammers and scalpers and advertisers. These privacy abuses

are leading to mental, physical, and financial harm, and the harms are well documented and in fact, some of the most vulnerable among us, including the elderly, veterans, and people of color.

But there are few things more concerning to me than the ways Big Tech, including data brokers, have proliferated the surveillance and targeting of our kids. Take Recolor. Recolor is an online coloring book operated by KuuHubb. Recolor provides images that consumers can color in on their mobile devices, including kid-friendly images like animated characters and cartoons.

In 2021, KuuHubb was found to have collected and disclosed personal information about children to third parties, including advertisers, without their parents' consent. Like so many others, this company enticed children onto their platforms only to monetize their data for the company's own commercial benefits.

Furthermore, in 2021 a data broker called OpenX was fined $2 million after collecting personal information about children under 13, opening the door to massive privacy violations and predatory advertising. We know that Big Tech

has enabled advertisers to target children for a whole range of damaging products, ranging from tobacco and e-cigarettes to low-calorie diets that can create and exacerbate body image anxieties. Data broker profiteering is excessive, and it is this shameful collection, monetization, and selling of data on our kids that gets me so animated.

The U.S. now -- we have fallen too far behind in prioritizing the protection of all people online, but especially young people. Because we do not have a national data privacy standard, we are currently stuck with this patchwork of state laws and narrow protections that leave a wide swath of our neighbors vulnerable to privacy abuses, including by data brokers.

Fortunately, there is much that Congress can do. This week I plan to reintroduce my landmark Kids Privacy Act to keep children safe online and curb the power of companies to indiscriminately track and target children.

I also strongly support the bipartisan American Data Privacy and Protection Act, which would bring much-needed transparency to the brokerage industry, and minimize the data available for them to collect.

As ranking member of this subcommittee, I am committed to holding accountable data brokers that infringe on our rights. This is especially true for those who seek to profit from our kids over their best interests and the concerns of their parents. So I am glad we are doing this critical work on a bipartisan basis, and I look forward to hearing from the panel today.

[The prepared statement of Ms. Castor follows:]

**********COMMITTEE INSERT**********

*Ms. Castor. And with that, I yield back.

*Mr. Griffith. I thank the gentlelady. Now I recognize the chair of the full committee, Mrs. McMorris Rodgers, for her five minutes for an opening statement.

*The Chair. Thank you, Chair Griffith, for convening this hearing about the role data brokers play in the digital economy, and thank you to our panel of witnesses here this this afternoon.

This is our fifth in our series of hearings this Congress across the Committee for strong data privacy and security protections for all Americans. Today we seek to expose and learn more about how pervasive and invasive the collection and selling of people's data has become.

Data brokers are harvesting people's data, selling or sharing it without their knowledge, and failing to keep it secure. A stunning amount of information and data is being collected on Americans: their physical health, mental health, their location, what they are buying, what they are eating. With more Americans than ever using apps and digital services, this problem is only getting worse. People have no say over whether or where their personal data is sold and

shared. They have no guaranteed way to access, delete, or correct their data, and they have no ability to stop the unchecked collection of their sensitive personal information.

We must continue our work for a national data privacy standard so that individuals can exercise their rights, businesses can continue to innovate, and government's role is clearly defined.

Today we explore ways that we have become just dollar signs for data brokers and Big Tech. We need a national data privacy standard that changes the status quo and ensures Americans regain control of their personal information. Right now there are no robust protections, and current privacy laws are inadequate, leaving Americans vulnerable. For example, during government-enforced COVID-19 lockdowns, GPS and mobile phone data collected by a data broker was used by the state to spy on Californians exercising their right to attend church services. It certainly raises questions of how data brokers aren't just violating people's privacy, but their civil liberties, as well. This is unacceptable, and it is more what you would expect out of the Chinese Communist Party's surveillance state, not in America.

Data brokers' days of surveilling in the dark should be over. People should trust their data is being protected. We are at an inflection point to ensure our personal information is responsibly collected, especially since this data may be used to train or develop artificial intelligence that may or may not align with our values. We need to ensure that the metaverse doesn't become the next frontier for exploiting our kids. That requires a broad, comprehensive bill that will address all Americans' data, and put even stronger guardrails around our kids' information.

That is why the American Data Privacy and Protection Act included the strongest Internet protections for children of any legislation last Congress. And privacy protections should not stop with kids. We need a Federal privacy law that gives everyone data protections, no matter where they live and no matter their age. We will continue to build on our work from ADPPA this Congress, and get the -- these strong protections for kids and all Americans signed into law.

Thank you, Ranking Member Pallone and my colleagues across the aisle for continuing to work with us on this. I

look forward to today's hearing as we continue to explore how data collectors and brokers are manipulating our lives and our security.

[The prepared statement of The Chair follows:]

**********COMMITTEE INSERT**********

*The Chair. Thank you. I yield back.

*Mr. Griffith. Thank you, Madam Chair. I now recognize Mr. Pallone, the ranking member of the full committee, for his five minutes of an opening statement.

*Mr. Pallone. Thank you, Chairman Griffith and Ranking Member Castor.

This is an important hearing, as the committee continues its bipartisan work to protect people's privacy online by addressing privacy abuses in the unregulated technology sector.

Today we are examining data brokers. Most Americans don't even know what a data broker is, but they would likely be shocked at just how much personal information these brokers have compiled on each and every one of them.

Data brokers are companies that collect and market troves of personal information about American consumers. The data broker industry exists on collecting more and more data, and selling it to nearly any willing purchaser. In 2014 the FTC reported that data brokers collect and store information covering almost every U.S. household and commercial transaction.

One broker possessed information on 1.4 billion consumer transactions; another data broker's database covered $1 trillion in consumer spending; a third had 3,000 separate pieces of data for nearly every consumer in the entire country. This is more than $200 -- this is more than a $200 billion industry that continues to rake in massive profits year after year on the backs of consumers. And as you can imagine, this has resulted in serious abuses and infringements of Americans' privacy.

And there is a reason most Americans have never heard of data brokers, because the industry operates in the shadows of the technology industry, with virtually no transparency as it profits from the mass collection of our personal information. And what makes data brokerage particularly problematic is that, unlike platforms like Facebook and Twitter, data brokers rarely interact with consumers at all. Consumers do not provide data directly to brokers, and that is why most consumers have no idea that these brokers exist or what information these brokers have about them. That is extremely troubling, considering that these brokers collect highly-sensitive personal data like health information and precise

geolocation data that identifies a consumer's location within 18 feet.

Now, how exactly do brokers get this information? Well, we know that they scour the Internet for data on consumers' bankruptcy records, property records, criminal records, headers from credit reports, web browsing activities, and other details of consumers' everyday interactions. The data brokers also use hidden tools like software development kits and tracking pixels embedded in consumer cell phones and in the websites we visit to monitor online behavior.

But that is not all. Based on this raw data, these companies also make inferences about consumers, lumping them into a number of categories based on where they live, their ethnicity, their income, or even by projected health care spending. And with this data, companies can target children with manipulative advertisements, or create people-search products that can lead to stalking, harassment, and violence.

Data brokers also sell information to scammers, including those that target the elderly with bogus sweepstakes and technical repair scams, and that market sham businesses, educational or investment opportunities to

veterans.

And it is no wonder the American people don't think they have any control over their online data today. While there are some limited protections for children's health and credit data, these laws have left us with a patchwork of protections that leave large swaths of our private information available for Big Tech's profiteering.

So thankfully, this committee has taken the lead to rein in these invasive practices, and to give people back control of their information.

First we need to pass a national comprehensive privacy bill. I think we all agree on that. This would create a national data privacy standard and stop unrestrained collection of personal information on consumers by both Big Tech and data brokers.

And our legislation also finally shines light on the shadow world of data brokers by requiring them to register with the FTC. This will provide consumers with a single mechanism to direct all data brokers to delete the personal information they have already collected, and to opt out of further data collection by all registered brokers.

So second, we have to make sure that the FTC continues to receive the funding necessary to carry out its work and has its Federal court authority restored and improved. And these important steps would both provide transparency into this industry and restrain the collection of unnecessary data.

So I look forward to hearing from the experts today. But, you know, I did want to say, if I could, that when I mentioned some of these scams -- you know, I think I mentioned targeting the elderly with bogus sweepstakes, technical repair scams, market sham, educational investment, opportunities for veterans. -- I am just not mentioning these in a general sense. A day does not go by without somebody calling my district office and talking about how they have been scammed. So this is real. This is -- you know, this this we hear in our district offices and from people on the streets.

[The prepared statement of Mr. Pallone follows:]

**********COMMITTEE INSERT**********

*Mr. Griffith. So thank you, Mr. Chairman. I yield back.

*Mr. Griffith. The gentleman yields back. That concludes the members' opening statements.

The chair would like to remind members that, pursuant to committee rules, all members' written in written opening statements will be made part of the record. And please make sure you provide those to the clerk promptly.

I want to thank our witnesses for being here today and taking the time to testify before the subcommittee. You will have the opportunity to give an opening statement, followed by a round of questions from members.

Our witnesses today are Professor Laura Moy, faculty director, Center on Privacy and Technology at Georgetown Law Center; Marshall Erwin, vice president and chief security officer of Mozilla; and Justin Sherman, senior fellow and research lead for data brokerage project at Duke University Sanford School of Public Policy. Thank you all very much for being here, and we do appreciate it greatly, because this is how we learn, and how we can then work together to make good legislation.

Now, witnesses, you are aware the committee is holding this as a part of our oversight hearing. And when doing oversight hearings, we have the practice of taking testimony under oath. Do any of you have an objection to taking testimony under oath?

Seeing that no objection is presented, we will proceed.

The chair also advises you that you will be advised by counsel, or that you have the right to be advised by counsel, pursuant to House rules. Do any of you desire to be advised by counsel during your testimony today?

All right. And all three have responded in the negative.

Seeing none, please rise and raise your right hand.

[Witnesses sworn.]

*Mr. Griffith. And all three witnesses answered in the affirmative.

You are now sworn in and under oath, and subject to the penalties set forth in title 18, section 1001 of the United States Code.

With that, we will now recognize Ms. -- Professor Moy for her five-minute opening statement.

TESTIMONY OF LAURA MOY, ASSOCIATE PROFESSOR OF LAW AND FACULTY DIRECTOR, CENTER ON PROVIACY AND TECHNOLOGY, ON BEHALF OF GEORGETOWN LAW CENTER; MARSHALL ERWIN, VICE PRESIDENT AND CHIEF SECURITY OFFICER, MOZILLA; AND JUSTIN SHERMAN, SENIOR FELLOW AND RESEARCH LEAD, ON BEHALF OF DUKE UNIVERSITY, SANFORD SCHOOL OF PUBLIC POLICY

TESTIMONY OF LAURA MOY

*Ms. Moy. Thank you so much. Good afternoon to both the chairs and ranking members of both the subcommittee and the full committee. I am really grateful for the opportunity to testify today on this important issue.

So in 2018, CNN published a story about a man named Kip Koelsch who noticed that his 84-year-old father was receiving mountains of scam email every week. And then his dad called to tell him that he had won a Mercedes and $1 million. And it turns out that for years his dad had been spending money, thousands of dollars, on supposed fees for prizes that he had been scammed into thinking he had won.

Now, Mr. Koelsch's problems -- or his father's problems

-- probably originated with data brokers. He probably ended up on what is known as a suckers list. After a person falls for a scam once, they may end up on other suckers lists, categorized by areas of vulnerability such as sweepstakes lovers. And this is not an isolated incident. The Justice Department actually recently brought cases against multiple data brokers, alleging that over the course of several years they had refined and sold lists of millions of elderly and otherwise vulnerable individuals to scammers. In one instance, the company was aware that some of its clients were even defrauding Alzheimer's patients, and yet continued to let it happen.

So I hope this story has your attention as we talk about data brokers today and think about what is at stake. There is three points that I would like to highlight.

So first, data brokers hold tremendously detailed information about all of us. In the story about Mr. Koelsch, data brokers were maintaining lists of people who might be vulnerable to scams, but data brokers also deal in other more revealing types of information: health information; visits to doctors; children's information; purchase history,

including of specific items; and information scraped from social media; even information that users have deleted.

Some data brokers also deal in detailed location data. A few years ago a team of journalists reviewed a data set containing locations from more than a million phones in the New York area, presumably information shared by apps that were installed on those phones, and they were able to use that location information to identify specific people. And they also explained how they could use that information to learn intimate details about those people's private lives, like where they worked, and where they lived, where they worshiped, and when they spent the night at another person's home.

Second, Congress has to act to protect us from data brokers because we individuals cannot do it ourselves. We are all aware that we are constantly generating digital information about ourselves as we go about our daily lives. Eighty-one percent of adults now say they have little or no control over the data collected about them by companies, and that number doesn't indicate acceptance or resignation. On the contrary, 79 percent of adults say that they are somewhat

or very concerned about how companies are using that data. That is why it is so important that Congress scrutinize this important issue, as the subcommittee is doing today.

And third, the booming data broker industry does real harm to real people. I have already talked about mass scams like the type that affected the Koelsch family. But let me touch on a few more examples. So in addition to fueling scammers, data brokers also expose private information to stalkers and abusers, to marketers of predatory products such as high-interest payday loans, and to malicious attackers who breach and mine data brokers' databases for nefarious purposes, including to sell to foreign entities or over the dark web to sophisticated fraudsters.

In addition, law enforcement agencies sometimes turn to data brokers to make an end run around the Fourth Amendment, one of our most fundamental civil liberties, purchasing information that they wouldn't be able to get through lawful order. So a few years ago it was revealed that the IRS had purchased access to large amounts of location data to fuel some of its investigations. And last fall researchers found that one broker that claims to have location data for over

250 million devices was selling to nearly two dozen agencies.

Also, data brokers might be contributing to locking people out of important job and housing opportunities due to historical data that is inaccurate or skewed by discrimination. For a variety of important eligibility determinations, including for housing and employment, decision-makers sometimes rely on scores provided by data brokers, often times without even knowing exactly what information is behind those scores.

And finally, data brokers put minors at risk when they deal in information about families and children. A few years ago researchers reported that one broker of student data was offering information about kids as young as two years old. And in 2021 it was revealed -- and I know this was mentioned, as well, in the opening statements -- it was revealed that a family safety app was selling kids and their families' locations to approximately a dozen different data brokers.

So these are just a few of the harms that I would highlight, but I look forward to your questions. Thank you.

[The prepared statement of Ms. Moy follows:]

504 **********COMMITTEE INSERT**********

505

*Mr. Griffith. I thank you very much, and now recognize Mr. Erwin for his five minutes of opening statement.

TESTIMONY OF MARSHALL ERWIN

*Mr. Erwin. Chair Rodgers, Ranking Member Pallone, Chair Griffith, and Ranking Member Castor, thank you for holding this hearing today on such an important topic.

My name is Marshall Erwin. I am the vice president and chief security Officer at Mozilla.

Mozilla is a unique public benefit organization and open source community owned by a non-profit foundation. We are best known for the open source Firefox browser, which is used by hundreds of millions of people around the world. Privacy is an integral part of our founding principles, which state that individuals' privacy and security online must not be treated as optional.

The Internet today is powered by consumer data. While that data has brought remarkable innovation, it has also put consumers at direct risk. Many of the harms we see on the Internet today are in part a result of pervasive data collection and the underlying privacy threat. The targeting and personalization systems in use today can be abused, resulting in real-world harm to individuals and communities.

These targeting and recommendation systems are powered by data, data that is often sold or shared by parties that shouldn't have that data in the first place.

Now, at Mozilla we believe the Internet can do better. A huge amount of the work that we do focuses on building protections into the browser itself to prevent data collection in the first place. And if we are able to prevent that data collection, it never gets to the actual data broker. So we specifically work to protect consumers' browsing activity. This is the data that you create as you navigate from website to website. It can be incredibly sensitive, provide a really detailed portrait of your online life, which is why we work quite hard to protect it.

So we work, for example, to block what we call cross-site tracking. Or sometimes you will hear this referred to as cookie-based tracking. In 2019 we enabled something called enhanced tracking protection that blocks this in the Firefox browser. We turn that on by default, because we believe consumers cannot be expected to protect themselves from threats that they don't even understand or see.

Now, despite this progress, huge privacy gaps still exist. We know from our experience in Firefox that we can't solve every privacy problem with a technical fix. Dark patterns, for example, are pervasive across the software people use. Consumers are being tricked into handing over their data with deceptive design patterns, and that data is then used to manipulate them.

Once a consumer has been tricked into handing over their data, that is where the data broker comes in. And while browsers have some visibility into online tracking, we lose that visibility entirely once the data lands on a company's servers in a shared on what we sometimes call the back end. Companies may then share or sell that data for eventual use by other parties. This type of back-end data transfer is something that browsers and consumers cannot see. And because it is -- because of this limited visibility, it is nearly impossible to fully understand the extent of this data selling and sharing.

As a browser -- as browsers move to clamp down on the leading forms of online tracking, parties are increasingly using other forms of tracking and back-end data sharing and

selling. For example, we are concerned about the growing use of identity-based tracking. Often when you visit a website, you are encouraged to create an account and hand over your email address when you create that account. What many consumers do not realize is that their email address may then be handed over to other parties, including data brokers, that may then use that to build a profile of their browsing activity.

Lack of privacy online today is a systemic problem. We therefore believe that law and regulation have an essential role to play in the passage of strong Federal privacy legislation is critical. We supported the American Data Privacy and Protection Act in the last Congress, and are eager to see it advance in this Congress.

ADPPA defines sensitive data to include information identifying an individual's activity over time and across third-party websites and online services. This is incredibly important. Regulatory regimes need to move beyond narrow categories of what is traditionally referred to as PII. Browsing data must be protected both by the platforms that people use, like Firefox, and also by the regulatory regimes

intended to protect privacy.

I will close by noting this is actually the 25th anniversary of Mozilla's founding. So we have been working to protect our consumers for 25 years. We established the first bug bounty program almost 25 years ago, the first company to encrypt our users' web traffic.

Unfortunately, the privacy regulation has not kept up with this progress, and it is time for federal privacy -- federal policy to step in and protect consumers.

Despite being a powerhouse of technology innovation for years, the United States is behind globally when it comes to recognizing consumer privacy, and protecting people from indiscriminate data collection, use, sharing, and selling.

We appreciate the committee's focus on this vital issue, and look forward to continuing our work with policymakers to achieve meaningful privacy reforms. Thank you.

[The prepared statement of Mr. Erwin follows:]

**********COMMITTEE INSERT**********

*Mr. Griffith. I thank the gentleman. I recognize Mr. Sherman for his five-minute opening statement.

TESTIMONY OF JUSTIN SHERMAN

*Mr. Sherman. Chair Griffith, Vice Chair Lesko, Ranking Member Castor, and distinguished members of the subcommittee, I appreciate the opportunity to testify about data brokers and threats to Americans' civil rights, physical safety, and national security.

I am a senior fellow at Duke University's Sanford School of Public Policy, where I run our research project on the data brokerage ecosystem, the virtually unregulated, multi-billion dollar ecosystem of companies collecting, aggregating, and selling data on Americans.

Data brokerage threatens Americans' civil rights, consumers' privacy, and U.S. national security. While I strongly support a comprehensive privacy law, Congress need not wait to resolve this debate to regulate data brokerage.

Today I will make three points: Congress should first strictly control the sale of data to foreign companies, citizens, and governments; ban the sale of data completely in some categories, such as with health and location data and children's data, and strictly control the sale of data in

other categories; and third, stop data brokers from circumventing those controls by inferring data.

Our research at Duke University has found data brokers advertising data on hundreds of millions of Americans, including their demographic information, political beliefs, home addresses, smartphone locations, and health and mental health conditions, as well as data on first responders, students, teenagers, elderly Americans, people with Alzheimer's, government employees, and current and former members of the U.S. military.

Data brokers can track and sell your race, religion, gender, sexual orientation, income level, how you vote, what you buy, what videos you watch, what prescriptions you take, and where your kids and grandkids go to school. This harms every American, especially the most vulnerable. And I will give three examples.

Data brokers sell sensitive data on members of the U.S. military. Criminals have bought this data and used it to scam service members, including World War II veterans. Foreign states could acquire this data to profile, track, and target military personnel. The Chinese Government's 2015

hack of the Office of Personnel Management was one of the most devastating breaches the U.S. Government has ever suffered. But there is no need for the Chinese Government or any other foreign state to hack many databases when so much data can be bought on the open market from data brokers.

In a forthcoming study, our team at Duke purchased individually identified data on military service members from data brokers with almost no vetting and as low as 12.5 cents a service member. Data brokers known as People Search Websites aggregate millions of Americans public records, and post them for search and sale online. Abusive individuals for decades have bought this data to hunt down and stalk, harass, and even murder other people, predominantly women and members of the LGBTQ-plus community. There is little in U.S. law stopping data brokers from collecting and publishing and selling data on survivors of gendered violence.

Government personnel are at risk, too. In 2020 a violent individual bought data online about a New Jersey Federal judge and her family. He then went to her home, shot her husband, and shot and killed her 20-year-old son.

Data brokers also advertise data on Americans' health

and mental health conditions. Companies can legally buy this data from data brokers, and use it to target consumers such as teens suffering from depression.

Data brokers have also knowingly sold data on elderly Americans and people with Alzheimer's to criminal scammers because they made money off the sale, who then stole millions of dollars from those people. Foreign governments could even use this data to target government personnel.

Our research has found that companies selling this data conduct relatively little know-your-customer due diligence, and often have very few controls, if any at all, over the use of their data.

There are three steps Congress should take now.

First, strictly control the sale of Americans' data to foreign companies, citizens, and governments, which currently can entirely legally buy millions of U.S. citizens' data from U.S. data brokers.

Second, ban the sale of data completely in sensitive categories, such as with health data and location and address data, which can be used to follow, stalk, and harm Americans.

Third, stop companies from circumventing those controls

by inferring data, using algorithms and other techniques to basically derive information that they haven't technically collected.

Congress can and should act now to regulate data brokers and their threats to civil rights, consumers' privacy, personal safety, and national security. Thank you.

[The prepared statement of Mr. Sherman follows:]

**********COMMITTEE INSERT**********

*Mr. Griffith. Thank you, and I appreciate your testimony.

Seeing there are no further members wishing -- got too far ahead in my script.

[Laughter.]

*Mr. Griffith. I now recognize myself to begin the question-and-answer section. I recognize myself to start that with five minutes of questioning.

Mr. Sherman, you got my attention.

[Laughter.]

*Mr. Griffith. Infer data. So what kind of information would they infer -- if we block the others and they start to infer data, what are we talking about there? Inferring that I live in a particular town? Inferring that I live on a particular street? And how do they do that?

*Mr. Sherman. Inference is one of the three main ways that these companies get data. So it is a huge data source for data brokers.

Inference might be something really basic. For example, do you have a Christian prayer app on your phone, or a Muslim prayer app on your phone? And that single data point can be

used to understand something so sensitive as an American's religion, something that they may never have inputted into a form, all the way to more sophisticated things. If you have location data, if you can follow people as they visit medical facilities, divorce attorneys, you name it, you can also from that derive information about them that they similarly have never typed into a form, and have no expectation is out there, but then that is put into these data sets for sale.

*Mr. Griffith. And do all the companies -- or are all the companies out there doing that, and do some of them just keep the data for themselves?

As an example, Sunday morning I am going to church, boom, pops up, Google tells me how long it is going to take me to get to church, because it is Sunday morning and I am pulling out of the driveway. I haven't asked them to tell me how long it is going to get to church, or what the directions are, but it just offers it to me. Is that part of what we are talking about, or is that considered acceptable?

*Mr. Sherman. I think that is what we are talking about, right? What can you learn about people based off location data?

As you said, different kinds of companies collect that for different reasons. A ride app might collect it because they need to know where you are to send the car, versus a data broker wants to collect that so they can profit off selling it.

*Mr. Griffith. All right. And, you know, we have talked about it. And for everybody watching, if I type in my email address, if I am shopping for something or if I decide to buy something -- and mostly that would not be me, but other members of my family -- and I do it for -- put down the address, the website, my email, put down my address so I can get it shipped, what is the chain of custody to the data broker and beyond? And where does my email address end up, or even my street address?

*Mr. Sherman. This is another main source for data brokers. There is a lot of what we will call first-party collectors, right? The one that the consumer directly interacts with -- as you said, an app or a website -- will then turn around in some cases and sell that directly to a data broker, or sometimes they will share it with advertisers. And then that enters an equally opaque

sometimes system where data brokers can get the information from there.

*Mr. Griffith. All right. So how do we craft legislation that protects that, but at the same time gives me the opportunity to actually let somebody know my location?

For example, many of the members of the committee know I am an avid bird watcher. So when I am out birding, I have several different apps. And, you know, if I am in a location, I want them to know where I saw that bird, so that other people can go see the bird. I want them to share that information.

How do we craft legislation that protects the privacy, but allows me to say, okay, I spotted the particularly rare bird or an unusual bird in Virginia at a certain location, and I want other people to know that? How do we protect it, but also allow it when I want to share my location?

*Mr. Sherman. As mentioned, I strongly support a comprehensive privacy law. I think giving consumers more control over what data is collected would help with that. So would controls specifically targeted at the sale of data.

As mentioned, it is not just data brokers who sell this

data. Sometimes the way they get it is a weather app or other app selling location data without people knowing it. And so that is also part of this system you mentioned, where that then gets out there for sale.

*Mr. Griffith. And part of what I have always envisioned -- and we will have to craft the legislation appropriately -- is that, as opposed to the small print that goes on for -- you know, I am scrolling down, down, down -- I used to read those. I have gotten numb like so many others, and I am just like, okay, I want to get this done. How can we get a box that just says, okay, you can share or you can never share, something simple that we can click on?

*Mr. Sherman. I think you just said it. It needs to be simple.

You know, data brokers, among others, hide behind this completely bad faith nonsense argument that people read privacy policies. I don't read privacy policies for everything I use, right? We don't have the time.

And so making that simple so someone can actually read it and understand it is really, really essential.

*Mr. Griffith. All right. I appreciate that. My wife

always used to make fun of me when I would read those privacy notices, and I did it for years. But I have given up. I appreciate your testimony and I yield back.

And now I recognize Ms. Castor, the ranking member, for her five minutes of questions.

*Ms. Castor. Well, thank you. And thank you again to our witnesses for your outstanding testimony.

So you have provided some very stark examples, Mr. Sherman. Can you dive into the kids privacy for a minute, and give us an example?

There is a minimal privacy law on the books. COPPA was adopted in 1998. The world was entirely different then, but they still collect vast amounts of data on kids and use it to exploit them. Give us an example so we can focus on the harm.

*Mr. Sherman. I would put these issues around children's data and data brokers into two categories. So I will give an example.

So our team, through our research ethics process, also buys data from data brokers to understand the privacy risks. We recently asked a data broker, "Could you sell us'' because

they said they had some data on children. They told us no. They cited COPPA. But they said, "We could allow you to get information on their parents.'' And so that is not covered. That is something you could use to target a household, knowing there is maybe a certain number of children in that household, or children with a certain condition in that household. So there is that question of the controls there.

The second piece is COPPA only focuses on children under the age of 13. And so there is a massive market. You can go buy it right now of, literally, lists on 14 to 17-year-olds sold by data brokers out there on the market. And so targeting that, I think, is a key part of this, as well.

*Ms. Castor. Right. Dr. -- or Professor Moy, you also are very well familiar with COPPA. It says they have to maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information. But that is not happening, is it?

*Ms. Moy. No, no, I don't think at all. Nor there is also a prohibition in COPPA that services not collect more information than is reasonably necessary from a child to provide the site or service. And I don't think that that is

happening, either.

*Ms. Castor. So we have the ability in the law to put some guardrails, to adopt some guardrails. What about -- could we, in the law, say that there are certain time limits on information that is gathered, and after a certain timeframe it has to be deleted?

*Ms. Moy. I absolutely think that that would be a good idea.

I mean, I think that one of the things that many people don't quite understand about the information that they generate about themselves as they go about their daily lives is that that information can live forever, even after they think that they have deleted it from a site or service. Once it has been collected by a data broker, it might exist in databases forever.

And so I absolutely think children lack the capacity to consent. Often times their information is not provided directly by them, but in fact by their parents and families. And there should be a retention limit on information that is collected.

*Ms. Castor. And just like Mr. Erwin highlighted how

Mozilla has built into their browser design from the very get-go certain enhanced tracking protections to an encryption, we could do that in the law, couldn't we?

We could set guardrails, Mr. Sherman, on -- in addition to time limits on privacy settings, default -- just what Chairman Griffith said, it is default private first. And people have to have some kind of meaningful consent in to share, and we can have time limits around that. Is that right?

*Mr. Sherman. That is right. And kids is such an important category to protect that I think there is even more reason, as you are saying, to do that focused on children.

*Ms. Castor. There is no law right now that prohibits these data brokers from selling this data to malign foreign actors whatsoever?

Okay. I hear you loud and clear. We have a lot to do on this. So, Mr. Erwin, how -- why have you all decided in the wild, wild West of data to remain committed to online privacy? That is not in your -- that is not profitable for you. Or is it profitable for you?

*Mr. Erwin. It is not as profitable as we would like.

You know, I think the reality is privacy is so opaque that it doesn't -- the privacy properties that we built into the browser don't drive consumer awareness or action as much as we would like.

We build these things into the browser because we know fundamentally people need to be able to trust the platforms that they are using in order to engage online. And so, while they might not know in -- like, in detail exactly who is collecting their data, they are going to know that Firefox or the platform they are using is trustworthy. And that is something that we find to be valuable. It doesn't, like I said, drive our business interests as much as we would love, but it is something that we take very seriously.

Some of the other major platforms I think have moved sort of in lockstep with us, particularly, I would say, like, Apple's privacy protections are also quite strong, and applaud some of the steps they have taken. That covers roughly half of the browser and mobile operating system market. However, the other half, the average consumer uses of the other platforms, are still not benefiting from some of these core protections, and they are still -- their privacy

is --

*Ms. Castor. Thank you very much.

*Mr. Erwin. -- is still in jeopardy.

*Mr. Griffith. The gentlelady yields back. I now recognize the chairman of the full committee, Mrs. McMorris Rodgers, for five minutes of questioning.

*The Chair. Thank you, Mr. Chairman, and I appreciate you inviting everyone to be here today, and your testimony. And I wanted to start with an issue that has been debated for many years, and that is targeted advertising.

So, Mr. Erwin, I just wanted to start with you, and ask for you to give us some insights as to the ways websites collect data on users and the life cycles of that data.

*Mr. Erwin. Yes. So targeting -- targeted advertising really drives a large amount of the Web ecosystem today.

You know, roughly sort of a decade ago, targeted advertising was much more simple, and it seemed to power the Web just fine. So you had things like advertising for your average sort of news platform that you visited. It seemed to generate a fair amount of revenue for that platform, yet it wasn't nearly as sophisticated as it is today in terms of

being able to draw on deep profiles of data, some of that data being collected offline and shared with ad tech platforms, and some of it being collected online and shared with ad tech platforms. Once you have that really rich profile of data, that then allows the -- whatever site that you are using to draw on that data, to target ads to exactly the target audience that they want.

And the challenge is that that opens up really serious concerns for abuse, because the more you know about someone, the more you can manipulate them. You can target your message to exactly who you want. And in some cases, that can be fine if you are sort of making a standard sort of consumer offering. But in other cases it can be terribly problematic.

*The Chair. And then would you speak to the life cycle of that data?

*Mr. Erwin. Yes. So I think that data is often sort of immediately actionable. So the data is collected. You will visit a site, you will -- the ad tech platform will see, oh, you visited that site, you put something in your shopping basket, and then a week later they see you again and say, hey, you never finished that purchase. We still know exactly

who you are. We still think that you we want -- you to buy that thing. You are going to see a targeted ad on a completely different platform. So that is sort of the immediate life cycle of the data.

However, that data is really valuable, and it can then leak in many other places to data brokers, to other programmatic ad platforms, and the data will live on for extended periods of time.

*The Chair. Thank you.

Mr. Sherman, I wanted to ask if you would just maybe give some more insights around this, because in your testimony you referenced how data brokers collect data on elderly, on Americans with mental health concerns, on teenagers. Would you just discuss in more detail how they use this information to target and harm vulnerable Americans?

*Mr. Sherman. There are a variety of things that data brokers do with data. So they will point out -- which they do, the -- some companies do things like fraud prevention, identity verification, all the way to essentially building these packages, these targeting profiles, if you will, on different subsets of Americans. So maybe that is 30 to 40-

year-olds in D.C. who like coffee. Maybe that is elderly Americans with Alzheimer's, and then seeing who they can sell that to to make a profit off of it.

And so, as you alluded to, in some cases that has included -- in many cases that has included data brokers selling to scammers because they get paid for it. And then, as Professor Moy testified, they get put on what are called suckers lists, and then used to be targeted for astrology scams or all kinds of other fraudulent activities.

*The Chair. Well, so last month we had a hearing with TikTok's CEO, Mr. Chew, and certainly concerns about how the data is being ultimately controlled, and its connection to the communist -- Chinese Communist Party. And so there is the national security concerns around TikTok. But would you speak to their ability to -- you know, speak to the Chinese Communist Party and other foreign adversaries' ability to collect American data by buying it from data brokers, either directly or indirectly?

And then do the data brokers have any protections in place to prevent this from happening?

*Mr. Sherman. We have not found in our work that

brokers often vet who they sell to. Hence the scamming example. Hence also there is absolutely a risk that a foreign actor could approach a company or lie to a company about their intentions, and buy a bunch of data on Americans.

We are also all familiar with the Equifax breach, right, when the Chinese military stole hundreds of millions of Americans' data. Equifax is a major data broker, and an example of what happens when a company with that much data is not properly protecting it. Now a foreign actor has all of that information on Americans that has been pre-compiled, pre-packaged, pre-sorted, and ready for targeting.

*The Chair. Yes. So lots of opportunities for manipulation and abuse.

Lots more questions, but I am going to yield back, Mr. Chairman.

*Mr. Griffith. Thank you, Madam Chair. I now recognize the ranking member of the full committee, Mr. Pallone, for his five minutes of questioning.

*Mr. Pallone. I just wanted to say, Chairman Griffith, that, you know, I just was -- found it so interesting, what you said about the bird watching, because I think that maybe

you, like me, you know, we are in a world, you know, a few years ago, where, you know, people would say, oh, there is where the bird is, why don't you go look at it, right, and you don't even think about the fact that somebody may do something nefarious with that information, because we are kind of naive about what is out there.

And so, if I could ask Ms. Moy, I mean, you did this tweet, and you were -- you know, and I think you said that people would be shocked by the type of information that was available. So why don't you tell us what would surprise Americans about the scope of the data that is collected about them by these data brokers?

*Ms. Moy. Yes. I mean, I think that -- I think there are a couple things that I would highlight.

So one is there are all kinds of things that people think of as sensitive information that they think is already protected by certain laws that is actually not within the scope of the laws that we have protecting those types of information.

So some examples are health information. A lot of people think like, well, we have a health privacy law. And

that is correct. But there is a lot of information that is collected outside the context of actual medical services that people would think of as health information: purchases of -- you know, I think I read in the 2014 Senate report about purchase information of yeast infection products and laxatives, that that was in a data broker file; information from wearable health devices; information about how frequently someone visited a doctor. That information -- people would expect that it is protected, but it falls outside the scope of our existing laws.

And then I think another thing that people would be really surprised about is that the information -- again, the information potentially lives forever. So people may think that something that they posted a while ago on a social media platform, like on Twitter, and later deleted is gone. But it is not. If it has been scraped by a data broker it may live forever.

*Mr. Pallone. And then this whole issue you wrote in your testimony, it says, "If well-informed individuals wanted to remove their own information from data brokers, as a practical matter it is nearly impossible.'' What does that

say about the amount of control that consumers currently have over how their data is collected?

*Ms. Moy. Yes, I mean, I think people really have very little control right now, as I think everyone on this panel has highlighted. This is a very opaque industry. Often times individuals don't have relationships with these companies.

And so -- but even when there is an opt-out, there are -- a couple of journalists have written about this, about their attempts to erase their own information. I have done it myself. It is really hard. One journalist described it as a labyrinthine process to try to opt out, and said that opt-outs are hard to find out about, much less navigate, and she pointed out that it is actually much easier to buy records about your neighbors than it is to scrub your own personal information from brokers.

*Mr. Pallone. Well, Mr. Sherman, in your testimony you talk about the same issue.

So what -- I mean, it seems to me what we really need is like a one-stop shop for consumers to use to request that data brokers delete information. And I know that the

comprehensive Federal privacy legislation which myself and Chair Rodgers and I think everybody on the committee has cosigned does have that kind of a mechanism.

So how would you -- what would you suggest about creating a mechanism that helps -- limits data brokers' power to profiteer, and restore control?

*Mr. Sherman. A one-stop shop would certainly help, right? Part of the issue now is consumers not knowing this is happening, and then having to go figure out which of 1,000 or so companies -- more than that -- to contact. And so having a one-stop shop to do that would be good.

The other thing I would add is that, with people search websites, where public records are scraped or home addresses are posted, the source of stalking, the source of the attack on the judge's home, in part -- those are often exempt from a lot of these bills and these state privacy laws that have been passed because they have broad carve-outs for publicly-available information.

And so I think that is another challenge, is to say yes, of course, we want public records out there. We are a democracy. We want things to be available. But we need to

recognize the immense risk to individuals by having that posted, as Professor Moy said, online for easy purchase.

*Mr. Pallone. Well, thank you so much. This panel is fantastic, and this hearing is so important.

Thank you, Mr. Chairman.

*Mr. Griffith. Thank you very much. The gentleman yields back. I now recognize the gentleman from Texas, Dr. Burgess, for his five minutes of questioning.

*Mr. Burgess. Thank you, Mr. Chairman. And again, fascinating panel.

Let me just ask -- sort of like asking for a friend.

[Laughter.]

*Mr. Burgess. What is the value of -- someone aggregates data and sells it to someone. What is, like, the cost per person? What is the return on investment there? Like, how much do you get per deliverable, per person's personal information? Is it like pennies? Is it like a dollar?

*Mr. Sherman. So often times brokers will not -- large brokers will not sell you a single person's information, but they will give you a data set, as you said, with a price per

record.

As mentioned in a study we have coming out, we bought individually identified data on military service members for as cheap as 12-and-a-half cents a service member. You can also buy lists of teenagers or people with Alzheimer's, and maybe it is $0.30 or $0.40 a person.

So even if you are buying a few thousand records, you are only spending a couple hundred dollars to get this information.

*Mr. Burgess. So several years ago there were a number of well-publicized data breaches and -- like for an insurance company -- and the comment was made, well, this was data at rest. This wasn't data that was actually being used for anything. What is the value of that to someone who then steals that kind of information? Are they able to monetize it and turn it around and make it a commodity that is for sale?

I guess, Mr. Sherman, I will stick with you.

*Mr. Sherman. It depends what is in the data, but it absolutely can be valuable. We know that, from various studies, that health information is some of the most valuable

sold on the dark web. You can buy that. As my fellow panelists mentioned, a lot of that is not covered by HIPAA. Companies are legally allowed to sell it.

Another example in the national security context, you can imagine location data or other information on government personnel that you could get and then could be used in a variety of ways.

*Mr. Burgess. Well, this committee, the subcommittee, had a very good hearing. Professor Moy, in her written testimony, talked about the scamming of elder individuals, and we had a -- quite an involved hearing on how elder abuse that was actually happening in that way. Is there a certain type of information that people go after to get at these -- at a list of people who might be susceptible to making these types of purchases?

*Ms. Moy. I mean, so I think, you know, these suckers lists often might contain information. Could just be contact information, but it might be information also -- detailed information about the types of scams or the types of solicitations that individuals had responded to in the past. And so that was certainly at issue in some of these cases

that the Justice Department brought.

Some of the brokers had been observing the types of solicitations that individuals responded to, and used that information to refine and further categorize users based on their particular vulnerabilities.

*Mr. Burgess. So, Mr. Chairman, I wonder if they actually compare to the birders list on that. Just a hypothetical question.

Mr. Sherman, let me just ask you on the health data, Federal protections for American citizens right now that are required of these brokers.

*Mr. Sherman. HIPAA is often referred to as the U.S.'s health privacy law. Sometimes it is easy to forget that the P in HIPAA for portability, it is not for privacy. And so there are privacy rules associated with it, but it only covers a narrow set of entities: hospitals, health care providers.

There are lots of apps, websites, particularly health and mental health apps, that exploded during the pandemic that are not connected to a covered entity, and therefore are not bound by HIPAA. The FTC has been shining a light on this

recently, as well.

*Mr. Burgess. So let me just ask you. And we have all done this. You buy a new wearable device, and you sign up for something. Is that in perpetuity? If I no longer use that health app, how long does that license exist?

*Mr. Sherman. If you are referring to the data, there is no limit on how long a broker could keep that information.

*Mr. Burgess. And so the data that is generated by a wearable, for example, is continuously accessible by whatever person you originally signed on with?

*Mr. Sherman. It depends on the specific device. As mentioned, some companies like Apple are more privacy protective. Others do not have those protections in place.

*Mr. Burgess. Fascinating discussion.

Thank you, Mr. Chairman. I will yield back.

*Mr. Griffith. The gentleman yields back. I now recognize the gentlelady from Colorado, Ms. DeGette, for her five minutes of questioning.

*Ms. DeGette. Thank you so much, Mr. Chairman, and I want to thank you and the ranking member for holding this important bipartisan hearing.

Mr. Sherman, both you and Professor Moy talked just a few moments ago about the fact that health care data is not protected, but people think it is protected. I am wondering if you can expand on what types of health care data are not protected.

*Mr. Sherman. As mentioned, it is less about the type of data and more about the source of the data. So there is health information that if you told your doctor they can't go shout it on the street corner, they can't write it up and sell it. But if you tell that to a certain app or website, they are allowed to do so. And so you can get data on Americans with depression, with anxiety, with PTSD. You can get information about the prescriptions that people are taking for sexual health conditions, mental health conditions. You can get data related to pregnancy, and fertility, and motherhood, and all kinds of things.

*Ms. DeGette. So -- and, of course, we expanded telehealth during the pandemic. So would that also expand to telehealth?

*Mr. Sherman. It often does. And many of the mental health apps that surged during the pandemic, whether that was

to set up appointments or do meditation, or --

*Ms. DeGette. Let me stop you for a minute. Mental health, but also physical health consultations. If somebody is consulting by telehealth with a doctor, that could also be vulnerable, that data.

*Mr. Sherman. If an app is connected to a HIPAA-covered entity, so if it is an app for a hospital, for example, that is covered.

*Ms. DeGette. Okay.

*Mr. Sherman. If it is outside of that, that might not be covered.

*Ms. DeGette. Okay. So basically, data brokers are collecting lists of people living with diseases and ailments like diabetes, depression, even women who are pregnant, and selling this information to people who can exploit the consumers. Is that right?

*Mr. Sherman. Yes.

*Ms. DeGette. Professor Moy, would you agree with that?

*Ms. Moy. Yes.

*Ms. DeGette. Now -- so are you aware, Mr. Sherman, that law enforcement agencies have purchased data broker

information on U.S. citizens, ranging from home utility data to real-time locations, even though the information may not be complete, current, or accurate?

*Mr. Sherman. Yes.

*Ms. DeGette. So all -- so theoretically, if a law enforcement agency can purchase this information, they could purchase any of the kinds of information we were just talking about.

*Mr. Sherman. Correct.

*Ms. DeGette. Right? It wouldn't be limited to, like, utilities or location. They could purchase any of this information about medical information.

*Mr. Sherman. Yes.

*Ms. DeGette. Now, have data brokers sold location information linked to specific devices that could track individuals' movements to reproductive health clinics and other sensitive locations that you know of?

*Mr. Sherman. There have been a few journalistic investigations on this indicating that they have. The question comes back to how identifiable is the data. It might not literally be a name, but I would say, yes, it can

be linked to a device.

*Ms. DeGette. It can be linked to that. Now, in your testimony -- or Dr. Moy, did you want to add to that? No?

*Ms. Moy. No, no.

*Ms. DeGette. Do you agree?

*Ms. Moy. I agree, yes.

*Ms. DeGette. Okay. In your -- now so, Mr. Sherman, in your testimony you recommended three steps that Congress could take to address this. I am wondering if you can hone that in specifically to health and location data that could protect American consumers.

*Mr. Sherman. I think banning the sale of health and location data is the best route to prevent those harms. As mentioned, health and location data are very sensitive. They can be used very harmfully. Both Democrats and Republicans agreed almost 30 years ago now with HIPAA that health privacy is important and must be protected. Location, similarly, is unique to individuals. You can also learn other things by following people around, as you mentioned. And so those, I think, are two really important categories to focus on.

*Ms. DeGette. Great. Well, thank you. And I look

forward to working with my colleagues on this, because it is almost inconceivable to us to see how far the tentacles of these intrusions go. But I think they can go in very, very bad ways.

And I yield back.

*Mr. Griffith. I thank the gentlelady, and agree, and now recognize the gentleman from Kentucky, Mr. Guthrie, for his five minutes of questions.

*Mr. Guthrie. Thank you, Mr. Chair. I appreciate the opportunity. Thanks for all the witnesses being here.

Mr. Erwin, in your testimony you refer to dark patterns, and you stated dark patterns, for example, are pervasive across the software people engage with daily. Consumers are being tricked into handing over their data with deceptive patterns. Then the data is being used to manipulate them.

So my questions are how are consumers being tricked into handing over their data? What are examples of these deceptive patterns? And are there technical fixes to prevent them?

*Mr. Erwin. Yes. So we heard earlier -- I thought the example of location data from the chairman was interesting

because, ideally, a consumer should be able to hand over their location to a party explicitly and have some value exchange. They are getting a service in return.

The challenge we see online today is you are handing over your location or your other data, and you might be giving that directly to the website you visit, and you know you are doing that, but you don't realize because there is some click-through box and some long, long text that you are never going to read, or some deceptive sort of always-on data collection button that you never realize is on, and therefore you are going to be sharing more data than you expect, or sharing it with parties that you don't expect. Those are the type of design patterns that we see across many of the websites that we all use on a daily basis.

*Mr. Guthrie. Are there technical fixes to that?

*Mr. Erwin. So I think one of the many things that I like in ADPPA is a call-out trying to define consent and establishing that manipulative design patterns that do not provide meaningful consent and try to trick consumers into consenting data collection without fully understanding are -- that is -- it is simply not an acceptable practice.

I think that is a good approach, and one -- like I said, one of the many things that I like in the draft.

*Mr. Guthrie. Okay. Yes, location data. For instance, there has been a couple of criminal cases, one in South Carolina, one in -- the horrible incident in Idaho, where the location on the person's phone -- you can't think of everything if you are going to cover your tracks. Your phone tells a lot of things you don't think about. And so it has been beneficial in some ways, but it certainly is concerning for us.

So you also say in your testimony we are reaching the limits of what we can do in the browser to protect people from this data collection. And so, as you were talking about, there is -- what are -- so I guess my question would be, why do you think we are reaching the limits?

What types of browser information can we protect, and what can we not protect?

And then what would be your message to websites and tech companies if they want to better protect their users?

*Mr. Erwin. Yes. So just historically, one of the interesting sort of arcs of narrative about privacy is it was

not built in early enough into your browsing experience in your -- in the browser, in the operating systems you use, in the mobile operating systems you use. And at least some companies have been very forward-leaning in trying to correct that early mistake.

And so we have done things like -- for example, we talk about deprecating cookies, or blocking what we call cookie-based tracking. This is the standard tracking mechanism online, historically, that has been used to build a profile of what you are doing on the Web. However, there are some underlying techniques that we know we can do much less about.

So one of these -- and just to go into the weeds for a moment -- we call browser fingerprinting. The basic idea, almost like a fingerprint that you have, is there are certain characteristics of your browser -- the screen size, for example; the fonts that you have installed in your browser -- that, actually, if you collect this data -- and it is data that is really critical to your usage of the browser, but it actually -- if you collect enough of it, it becomes a unique identifier that then follows you around. That is what we call a browser fingerprint.

And again, that is the type of thing which, like -- there were explicit identifiers, cookies, ad IDs that were built into platforms like the browser that we have removed, and that we have made real progress. But there is some things like this -- like I said, browser fingerprints that we can actually do very little about. We are working on it, but we know that it is a much, much more difficult space for us.

*Mr. Guthrie. Okay, thanks.

And I guess, Mr. Sherman, we had the TikTok hearing, and the TikTok CEO testified that he could not say with 100 percent certainty that the Chinese Government did not have access to American user data.

If you couldn't -- could the Chinese Communist Party get the same data by purchasing it if they get it just from TikTok, which they own?

*Mr. Sherman. It might not be all the same data, right? But you can get a lot just by buying it. Or if you are someone like the Chinese Government, just stealing it from the companies that are doing the work to precompile and package it.

*Mr. Guthrie. Well, so that is the question I was

getting to. So if we passed all kinds of privacy laws, but there is bad actors and bad players that own companies, they would still have access to the data, even if the law says you can't share this data, or it can't be submitted, or so forth. Correct?

*Mr. Sherman. There is always a risk of hacking. And so we do need to think about cybersecurity protections for all kinds of data alongside the privacy controls on them.

*Mr. Guthrie. Because we learned that -- a lot of these deceptive practices are -- people call me all the time and say, well, if it is a website from Russia, it is tough to prosecute, and those kinds of things. So we need to be aware that there is deceptive players all around.

My time has expired, and I will yield back.

*Mr. Griffith. The gentleman yields back. I now recognize the gentlelady from Illinois, Ms. Schakowsky, for her five minutes of questions.

*Ms. Schakowsky. I really want to thank the witnesses.

You know, for the purpose of this hearing, I think there is two things that we know. One is that most Americans worry about their data privacy, that -- and are concerned that it

is not being protected. And two, as has been said over and over again during this hearing, is that most consumers don't know a thing about, you know, the data brokers, who they are, what -- how it works.

So I wanted to call attention -- and this has been mentioned, too -- about our American Data Privacy and Protection Act in which we say that we would require all data brokers to register, essentially, so that we would -- everyone would have access to a list. And you could, with one push of the button, actually disconnect from that. You could, you know, take yourself out.

And I wondered how you think -- if this is an effective way to go, and that this would be a really important advance for consumers.

I just want to point out still I think we would have to educate people that this is going on. If they see the term "data broker,'' they still might not know what it is, but we would give them the opportunity to opt out. What do you think?

I would like each of you, if you have an answer, that would be great.

*Ms. Moy. I am happy to start. Yes. So I think -- I mean, a registry would certainly be a good place to start, as well as a one-stop shop for people to opt out. Yes, the -- it is incredibly opaque right now. A registry would both help the Federal Trade Commission exercise oversight, help people gain some insight into what is happening. And a one-stop shop would be really important for opting out.

I think a few things to think about are what the incentive is to register. So right now I think the penalty is $10,000 for not registering in the bill, and that is something to think about, whether that is a sufficient penalty.

And I think a couple of questions that this approach raises also are what we do about first parties that are collecting tremendous amounts of information that maybe kind of are data brokers, but do have relationships with individuals, and what we do about publicly available information, which -- a lot of data brokers claim to be dealing entirely in publicly available information.

*Ms. Schakowsky. Thank you.

*Ms. Moy. But it is a very good start, I agree.

*Mr. Erwin. Yes, we support a combination of what we think of as universal opt-outs plus sort of default privacy protections.

So in some cases, the opt-out, especially along the lines of what you are suggesting, is really critical and valuable. There is similar opt-out mechanisms that people have proposed in your web browser so that you don't have to opt out from every website to website. So decreasing the opt-out friction is really critical, because it is so easy right now to hand over your data and really hard to prevent parties from collecting that data.

The one challenge with that, though, is we know that consumers typically aren't -- still aren't going to use a lot of these opt-out mechanisms. That is why it is also critical to have some baseline protections, prohibitions against data selling, default strong protections so that users don't always have to opt in. And in some cases that is actually a better outcome than leaning on opt-out mechanisms as the sole mitigation.

*Ms. Schakowsky. Before I get to you -- but I want you to answer this question, Mr. Erwin -- is there a really good

rationale for data brokers, period?

*Mr. Erwin. I will answer that one first. Again, as I mentioned, data brokerage covers a wide range of activities. So there are companies that will sell to employers and to landlords and say, "If you want to do income verification for someone you are looking to hire, give us their name, we will tell you what we have.'' There is still a privacy question about that, but it is all the way to, as mentioned, some really egregious cases where I think the case is really strong for regulation and not for allowing, for example, health data to be sold, right?

The marginal benefit, potentially, is someone gets marketed a product that they could use for health condition -- that is even then questionable -- all the way to, as we have seen, scamming people with Alzheimer's, and dementia, and things that are patently harmful.

*Ms. Schakowsky. And the idea of our language that we have in our bill?

*Mr. Erwin. Yes, I like it. I think it is a great first step. I would agree with what Professor Moy and Mr. Erwin said. I think thinking about enforcing the opt-out is

important.

There have been folks, as my fellow witness mentioned, who have tried to get their name taken off these people search websites. They might opt out. The company might say, okay, we will do it. And the next day their name is back on there, because it repopulates or because, if you click on my sibling, then my page pops back up.

So making sure they are actually deleting that data, actually stopping the sale, I think, is the second big piece of that solution.

*Ms. Schakowsky. Great.

Thank you to all three of you. I appreciate it.

*Mr. Griffith. The gentlelady yields back. I now recognize the gentleman from South Carolina, Mr. Duncan, for his five minutes of questioning.

*Mr. Duncan. Thank you, Mr. Chairman, a really informative committee hearing.

This might be off topic, but are these things listening to us and sharing our data?

*Mr. Erwin. So it is interesting. In fact, they are not. But, you know, the major --

*Mr. Duncan. I mean, how can you say that? Let me preface it.

*Mr. Erwin. Yes.

*Mr. Duncan. You know, I may have a discussion with Kelly Armstrong about the beaches at Normandy and -- or the Battle of the Bulge. And then I go to a social media site and within seconds an ad will pop up on that topic. And it could be oriental rugs. It could be something that, you know, is just off topic that I normally wouldn't talk about, but because I did in a setting, ads pop up. And it happens too many times for me to think they don't.

*Mr. Erwin. Yes, it is pretty amazing, isn't it? I think it is even scarier, though, because what is really happening is many of the major tech platforms know so much about you that they can predict your behavior. They can predict your conversation.

*Mr. Duncan. They can't predict something like an oriental rug.

*Mr. Erwin. In fact, they can. That is -- it is remarkable, how sophisticated some of these companies are. And so that is actually what is happening. They are not

listening to you, but they have such incredible predictive power that they can figure it out.

*Mr. Duncan. I am going to say Hermes ties, and I will bet you at some point this afternoon I will have -- let's move on. I think they are, and I think it is scary, the amount of data --

*Mr. Erwin. It is, yes.

*Mr. Duncan. -- that these devices are collecting.

I was in the auction business, did real estate marketing, and I was able to buy MEL list using an OSC code, I think it was called, and did direct mail marketing to people I thought may want the property I was selling. Unsolicited mail pops up in your mailbox. How is this different than what marketing companies were doing then through buying those mail lists?

*Mr. Sherman. I can maybe start. I would say it is not entirely different, right? There are brokers who sell those kinds of marketing lists now.

I think the questions come back to the scale of the data collected, the depth of the data, as Mr. Erwin mentioned, that is out there.

And the third piece is are you actually vetting who you are selling to? As you mentioned, if you are perhaps doing marketing for your small business, that might be one thing. But there was a case where the Justice Department went after Epsilon, a multibillion-dollar broker that got sample scam mails that the criminal scammer was going to send to elderly Americans, and approved the sale anyway.

And so it comes back to that question of what are you actually doing to make sure that someone is not going to use that same information in a harmful way.

*Mr. Duncan. I yield to Armstrong.

*Mr. Armstrong. Well, I just have a secondary question to that real quick, and I agree with that. But even on its best scenario, right, I mean, even whether it is legitimate or illegitimate, there is still a difference between contextual advertising and actually targeted advertising. Like, if you are buying old mail lists and you are going to elderly people, that is not -- I mean, you are targeting a specific group in a contextual capacity. This is micro-targeting at a much more sophisticated and, quite frankly, dangerous level, right?

And I yield back.

*Mr. Sherman. Absolutely, yes. And you can buy lists that maybe are not just name and one column with interest in real estate. You could buy with health and all kinds of other things we have mentioned in that same data set to really, really get precise about targeting people.

*Mr. Duncan. Thank you for that. Let me just ask this. In your written testimony you talk about various state laws, including those in California and Vermont, that define and require data brokers to register with the state governments. There is also laws in Delaware, Michigan, Virginia, Colorado, and others.

Are these laws sufficient in protecting American privacy? Yes -- if yes, why? If not, why not? And then -- that is for you, Mr. Sherman.

Mr. Erwin, I would like to ask what would be the advantage of having a Federal law defining and regulating data brokers, as opposed to the patchwork of state laws?

*Mr. Sherman. I would say no on the registry laws. They are an important step, but they don't do anything to block the sale of data. They force some companies defined

narrowly to register. A lot of that information actually is wrong or outdated. And so we do need to do more on that front, such as actually controlling the sale of data in regulation.

*Mr. Erwin. Yes, we think the Federal law is really critical.

The challenge with state law is, one, it is going to leave a large number of people unprotected where those laws haven't passed. And that, to us, is the biggest problem. A lot of Americans today aren't going to benefit from the privacy protections in CCPPA (sic), for example.

The other challenge with having a patchwork of state laws is, you know, when your legal team looks at that, and you see this complexity of the regulatory environment, it kind of looks for, like, the bottom line. What is the minimum? And the challenge -- and that is really not good for consumers, either, because it means we are not setting a high bar that everyone can be held to. Rather, your legal team is just doing legal risk mitigation, and that is not a great situation to be in. It is not good for consumers, either. So the Federal law, to us, is much preferable.

*Mr. Duncan. I still think the phones are spying on us and sharing that information with some social media platforms until I am convinced otherwise.

And I yield back.

*Mr. Griffith. Many of my constituents would agree with you, Mr. Duncan.

That being said, the gentleman yields back and I now recognizes the gentleman from New York, Mr. Tonko, for his five minutes of questioning.

*Mr. Tonko. Well, thank you, Chair Griffith, and thank you, Ranking Member Castor, for hosting this hearing.

I think it is important to hear from you folks at the table, so thank you to our witnesses.

The data brokerage industry's practices are deeply intrusive. This industry monetizes personal data, including sensitive information like data on mental health and addiction. Americans already face many barriers to seeking out treatment for mental health and substance abuse without data brokers trying to exploit their condition for profit. So what people struggling with mental health and addiction need to know is that they are not alone, and that real help

is available.

So, Mr. Sherman, have you found that data brokers are capitalizing on the mental health crisis in this country to boost their profits?

*Mr. Sherman. I think so. The more that mental health services that are not regulated are collecting mental health data, the more they are able to sell it to data brokers.

*Mr. Tonko. Any -- do the other two witnesses have any comments on -- or any experience in knowing about any of the mental health community?

Okay. I understand that many data brokers collect data to feed targeted advertisements, including those directed toward vulnerable populations like those struggling with addiction. In February I introduced the Betting on our Future Act to stop sports betting's harmful advertising that preys on the estimated seven million people in the United States who have a gambling problem or addiction.

So, Mr. Sherman, how have you seen data brokers collect and market data on people struggling with addiction?

And how has that data been used by companies to capitalize on these given addictions?

*Mr. Sherman. As mentioned, some of the health data that is out there could include things like drug addictions. You can also go buy from data brokers data on gambling addicts, or data on people who -- and I am no medical expert or anything, but might not be addicts per se, but go to the casino a lot, for instance. So that stuff is out there for purchase.

*Mr. Tonko. Yes. Well, we heard from some individuals when we did a roundtable discussion in my district on this -- the gambling addiction. And, of course, people who were in, for example, 30 years recovery from gambling were targeted for that sports gambling, as were, however, those who were 10, 15 years in recovery from illicit drug addiction. So it is just amazing to me that they can target these vulnerable populations for the purpose of financial benefit.

Mr. Erwin, what should online platforms be doing to ensure that users' browsing history isn't exploited by data brokers and advertisers to fuel addiction?

*Mr. Erwin. Yes, I mean, it is a remarkable example of a much broader problem, which is, again, like the more you know about something, you know their vulnerabilities, it

becomes easy to exploit those vulnerabilities to financial gain.

One of the major things we have advocated for is disclosure of what we call bulk advertising libraries, the basic idea being, especially for the major platforms like Google and Facebook, you know, all of the ads that are surfaced there should be available for the rest of us to inspect, to do analysis on, and to figure out if this is happening and people are being harmed. We should have the means to identify that harm and do something about it.

But because all of this content right now is so targeted, it is also invisible to the rest of us who aren't getting, for example, gambling ads. I am not going to see a gambling ad, and many of you might not. That harm is only happening to that specific set of individuals, and they are not even aware it is occurring. And so those are the types of things that we would like to see, as well, bulk ad libraries being a good example of the type of transparency that is necessary to get ahead of the types of harms that you are identifying.

*Mr. Tonko. Interesting. Any other thoughts on that

from -- Ms. Moy?

*Ms. Moy. Yes, sure. I think I would just add that thinking about the vulnerabilities and the way that messages can be targeted to folks -- addiction is a stark example. But similarly, folks who are financially struggling can be targeted for predatory products.

Similarly, folks who are vulnerable to certain types of messages could be targeted, micro-targeted with certain political messages, could be targeted with any kind of messaging that someone wants to deliver to sway a group of people. And that is very concerning, as well, as a possible threat to democracy.

*Mr. Tonko. Well, it is kind of indicative of how difficult these situations become for people who are struggling and are in recovery. And to know that they were preyed upon by outside groups because of their past experience is kind of a cruel approach, really. So whatever we can do to fix that is certainly something that we should pursue.

Big Tech's preying on vulnerable populations, including people with addiction and mental health concerns, is deeply

troubling, especially at a time when we need to be lifting up, not exploiting those who struggle in America with any given addiction. So I thank you for drawing attention to these issues.

And with that, Mr. Chair, I yield back.

*Mr. Griffith. The gentleman yields back, and I now recognize the vice chair of the committee, Mrs. Lesko, for her five minutes of questioning.

*Mrs. Lesko. Thank you, Mr. Chair.

Mr. Sherman, have foreign governments obtained data on American military veterans?

*Mr. Sherman. I don't know. I can't say decisively one way or the other. I think the question is about risk, right? And risk always is a matter of possibility. And if this much data is this available, and we have seen brokers sell it in other cases where it is harmful, there is a real risk here.

*Mrs. Lesko. Thank you.

Mr. Sherman, do data brokers advertise to prospective clients that they have personal information on U.S. military personnel?

*Mr. Sherman. Yes.

*Mrs. Lesko. And what kind of information about U.S. military personnel do they advertise?

*Mr. Sherman. You can essentially purchase anything we have mentioned related to members of the military. That could be health data, that could be political data, that could be data on children in the home, that could be marital status, location data, even.

*Mrs. Lesko. Thank you.

To any of you, we have passed out of the House last Congress a data privacy legislation. We have heard from some business sectors, including small business groups, that they are worried that there will be unintended consequences, that they will lose business, and so on and so forth. Do you have any recommendations, or do you have any concerns about that, or have recommendations on how we can structure the data privacy legislation?

*Ms. Moy. I mean, I think that size thresholds can be helpful. However, I also think that there are good reasons to still place obligations on even small businesses to appropriately protect individuals' information. And Cambridge Analytica was a very small entity, and was able to

do a tremendous amount of harm. So unfortunately, it is an area that just needs responsibility.

*Mr. Erwin. Yes, I agree with all that. I would just add, you know, it is important to keep in mind, like, the Internet is a remarkably innovative place with low barriers to entry, and that will continue to be the case once Federal privacy legislation comes into existence. It will remain an innovative, good place for businesses to go and build their business.

And we have, I think, at Mozilla a huge amount of respect for the innovative capacity of the Internet. And you can take a big hammer to the Internet and it is going to keep going. So I think those arguments are a little bit overstated, frankly. And like I said, I have a large amount of confidence that it will remain an innovative place for businesses to engage.

*Mrs. Lesko. Good, okay.

Mr. Sherman, I like your idea to ban sale of location and health data at a minimum, and also sell -- and ban selling data to foreign entities. I think those are -- and I may be wrong, but it seems like a more direct way just to

protect very sensitive of data.

I do have -- since I have a minute and 40 seconds left, I have a question for you, if you know the answer. So, you know, when you use Uber, as most of us do in Washington, D.C., you have to turn on the location data, right? And so do you know if Uber sells that data, the location data?

*Mr. Sherman. I do not know that. I will say this is a challenge with tackling this issue is lots of apps don't really share data. They just want to keep it to themselves and use it for, as you said, business purposes for what they need it for. Others share it all over the place, and sometimes it is hard to tell and get more transparency into that ecosystem without regulatory levers to crack it open.

*Mrs. Lesko. Yes, I mean, I often get these apps that you -- it might pop up and say, "Do you'' -- "This will share data and have access to your camera, and your files,'' and blah, blah, blah, do you want to do it?

And I am like, well, if I am going to be able to use the app, I kind of have to do it, right? And so that is the problem, correct?

*Ms. Moy. Yes. I mean, that is definitely -- that is

one of the problems with brokers claiming that they have consent for some of the information that they have is that, as a practical matter, folks can't do that.

I would also just add about the location data point specifically. In the example that the chairman gave about a bird watching app, if that app is advertising-driven, then even if the app developer itself is not selling location data, if the app is sharing location data with an advertising entity that is also present on the app, then that entity could be sharing location information. So there are multiple ways that location information could go from your phone through an app to another entity.

*Mrs. Lesko. Thank you, and I yield back.

*Mr. Griffith. The gentlelady yields back. I now recognize the gentleman from California, Dr. Ruiz.

*Mr. Ruiz. Thank you.

Data brokers have been collecting data on consumers from apps and public records for many years, with real implications for Americans, particularly for historically disadvantaged groups. We know that brokers routinely compile and sell countless segmented lists of consumers based on

characteristics like income level, race, ethnicity, often without consumers even realizing it.

But that is not all. Brokers have callously lumped consumers of color into categories, and then they sell those lists for a profit. One broker, for example, created and sold a list of consumers that it titled, "Ethnic Second City Strugglers.''

Mr. Sherman, can you explain why data brokers are interested in collecting data on race and ethnicity?

*Mr. Sherman. They collect it because they can make money from selling it. And as you said, even if it is something very sensitive like targeting historically disenfranchised communities, economically vulnerable people, there probably is a company out there interested in marketing to those people, or maybe a scammer interested in targeting those people that is going to buy that data package.

*Mr. Ruiz. So data brokers also hold vast quantities of information that can be used to exploit vulnerable populations and discriminate against protected groups. Brokers have used their vast collection of data to insert themselves into potentially life-changing decisions such as

Americans' housing, credit, and employment.

Mr. Sherman, can you explain how data on racial and ethnic minorities could be used to discriminate against vulnerable communities?

*Mr. Sherman. There are many ways. As mentioned, there are, essentially, no ways for consumers to know that this is going on, and so there is no opportunity to potentially correct information that could be wrong. And so situations already laden with bias could have incorrect information further entered, all the way to we know that health insurance companies, for example, will buy information on consumers, including things like race, income, education level -- and yet again, another system with many, many gaps in access and quality of care, and it is hard to know what they are doing with it.

*Mr. Ruiz. Okay. Professor Moy, how have you seen brokers capitalize on the lack of meaningful regulation by using data on Black and Brown Americans in a discriminatory way, particularly in areas such as housing, employment, and service eligibility?

*Ms. Moy. Yes, so I think -- so the folks at the

organization Upturn have done a lot of really useful work on this. And one of the things that they have pointed out is that some data brokers collect information about things like eviction records, and then might roll that into scores that then are relied upon by, for example, landlords to make housing decisions.

Now, this makes a lot of -- this makes intuitive sense, but the fact of the matter is that in certain areas, more economically depressed areas, landlords might be much more likely to move directly to eviction proceedings when payments are -- when rent payments are late than in other areas. So as a result, the historical data is biased against people of color in economically disadvantaged areas. And when those scores are then relied upon -- provided by data brokers to make decisions, then unbeknownst to the landlords they might actually be making decisions in a way that is discriminatory.

*Mr. Ruiz. Mr. Erwin, so you have commented before on the use of sophisticated algorithms that can use personal data to discriminate against people based on race or gender. Could you speak a little more about what you have observed in terms of discriminatory data use, and what we should be aware

of as we try to address these issues here in Congress?

*Mr. Erwin. Yes. So the canonical example of this is just basic targeting. "Targeting'' is the term that we use for any advertisement. In this case, it is targeting towards particular demographics of housing and jobs, a practice that historically we would have said this just looks like redlining, it is illegal. But in an Internet context, it is easy to do and opaque to the rest of us. And it means that some demographics are going to see particular jobs or particular ads for houses, and other demographics are not. And that is a big problem.

*Mr. Ruiz. Well, thank you to our witnesses for shedding light on this critical privacy issue, which has deep implications for the civil rights of vulnerable communities in our nation.

I yield back.

*Mr. Griffith. I thank the gentleman for yielding back, and now recognize the gentleman from North Dakota, Mr. Armstrong, for five minutes of questioning.

*Mr. Armstrong. Thank you, Mr. Chairman, and I wish I had an hour.

We are far into this hearing, and I agree with the privacy concerns at this -- on these levels of everything. But I want to talk about the Fourth Amendment, because this is one of the places where I think we don't spend nearly enough time talking about it, and the Fourth Amendment has withstood listening devices, telephoto lenses, satellites, drones, location trackers. Currently, you know, Carpenter redefined third-party carrier. There is geolocation warrant cases going through the system. Side note: I don't know how a geofence warrant is legal -- constitutional, anyway. It is a general warrant, not a specific warrant, but that is a longer question. Facial recognition.

But we don't talk -- we don't have a long-enough conversation about what this means with data brokers. And we have seen it. We have seen it in our hearings. And it is not always DoJ, right? It is CDC, IRS. We have had people on election integrity talk about backdoors into voting machines. Even the SECURE Act. And when we are talking about TikTok, there is, in my personal opinion, too much potential government intervention into those things. And it can be things as specific and dealing with all of those

different issues that exist, or it can be something as innocuous as when you are using energy in your house, right?

It turns out there is a really good public safety benefit from knowing where everybody is, what they are doing, and who they are at any given point in time in any community across the country. And it is not just Federal law enforcement, it is state law enforcement and all of those different issues.

But, Mr. Sherman, in your testimony you advocate for strictly controlling the sale of data to governments, which includes state, local, and Federal law enforcement, right?

*Mr. Sherman. The reference in my testimony to government sale was vis a vis foreign governments. But I agree it is an important question, right?

*Mr. Armstrong. Well, I agree with foreign governments, too. I just don't want the U.S. Government to be able to purchase it on the third party if it would require a warrant, either.

*Mr. Sherman. No, no, I agree. I fully agree with that. I think, as you said, we have had, you know, years of conversations about how do we properly put legal evidence

barriers and other things in place to make sure law enforcement is not overstepping, is violating Americans' freedoms.

The fact that any law enforcement agency can end-run around that by buying whatever they want from a data broker with no warrant, I think, is a huge problem.

*Mr. Armstrong. Well, and the response back to us would be if I -- if Kelly Armstrong, a Member -- just a guy from North Dakota can buy this information on the civilian marketplace, why shouldn't law enforcement be able to buy it? And that is a -- I mean, I disagree with that response, but it is truly a valid response.

*Mr. Sherman. I would say neither law enforcement should be able to buy it without a warrant, nor the scammer running around targeting someone. And so I think that is a sort of circular argument that gets passed.

As you said, the question of government overreach, the question of what is the oversight of that level of surveillance, and the answer is there currently isn't any.

*Mr. Armstrong. Well, and I agree with that. I mean, and anything that would require a warrant on direct source,

being able to circumvent that from third party is something we should be very -- I mean, and we know this.

Various law enforcement groups have expressed concern about the ADPPA's effect on criminal investigations. And in September of 2022 they sent us a letter, and it says, "This legislation would also make common investigative tools unavailable or extremely limited. The ADPPA would likely complicate the private sector's ability to continue its ongoing efforts to cooperate and share voluntarily, share certain information with law enforcement.''

Law enforcement claims that data purchased from data brokers largely consists of publicly available information, meaning data brokers merely aggregate this data for law enforcement in a more efficient manner. Ms. Moy, do you agree with that statement?

*Ms. Moy. So I will just point out that, with both telephones and banking, we -- the Fourth Amendment -- the Supreme Court found that this information was not protected, and, in fact, that is what spurred Congress to act, right?

I mean, like, that was the situation with United States v. Miller, and that is why Congress passed the Right to

Financial Privacy Act. You know, so I think that certainly law enforcement has grown to rely on some of these methods, just as law enforcement during prohibition had grown to rely on wiretaps. And that will be a change. But it needs to happen. We need these fundamental --

*Mr. Armstrong. Well, and I think the courts have already shown -- I mean, I think this really is the next step in the U.S. v Carpenter third-party carrier, right?

I mean, the courts were very willing to change how they viewed "third-party carrier'' in the digital age. I mean, that --

*Ms. Moy. Absolutely.

*Mr. Armstrong. That ruling was limited to persistent tracking and geolocation data through hell site -- or cell site information, but I think the principle is the same. And --

*Ms. Moy. Absolutely.

*Mr. Armstrong. So, I mean, there has been a massive expansion of -- and the other answer is that I think we don't -- we still talk about the data collection. We have AI, ChatGPT, all of these different things. The amount of

information they can analyze in real time is the second conversation that we need to have about this, because it is a truly scary -- it is scary on the civilian market, and it is very scary when government is doing it, as well.

*Ms. Moy. Yes, and if I can just respond to that very briefly, because I think this is a response also to what Mr. Duncan was pointing out, yes, these analytical tools render the factual context fundamentally different. You know, maybe having a list of addresses on paper at one time was something that didn't give people much cause for concern.

Now those lists of addresses, historical address information, can be mined to learn information about people's relationships and their, you know, their religion and their habits. And the same with location information. It is very different with the analytical tools we have now and in the future.

*Mr. Armstrong. Yes, and that is before you get into profiling and all of these other things that are -- traditional things would have real civil liberty protections.

I am sorry, Mr. Chairman, I yield back.

*Mr. Griffith. I know you are passionate about it, and

I appreciate it, but we have got to move on.

I now recognize Mrs. Trahan of Massachusetts for her five minutes.

*Mrs. Trahan. Thank you, Chairman Griffith, Ranking Member Castro for -- Castor, excuse me -- for allowing me to waive on to this hearing.

You know, over a year ago I introduced the DELETE Act with Senators Cassidy and Ossoff. This bipartisan legislation would require data brokers to register with the FTC and delete all the data related to a consumer at the consumer's request.

Now I am glad that a similar provision was rolled into ADPPA. That is a great sign that both parties are fed up with the lack of control consumers have over their data that is being collected and sold by brokers. But without Congress requiring transparency, the best way that I have found to learn what data brokers are up to is on AWS. I mean, literally, on the Amazon Web Services data exchange there is thousands of data sets with personal information under categories like health data, financial data, automotive data, and all are available for sale.

Now, a lot of these data sets include loan balances and clinical trial participation. Some of their descriptions say that they are anonymized. We know that that is not necessarily true. Mr. Erwin and Mr. Sherman, you discussed in your testimonies the ways that data brokers use different persistent identifiers to connect data to an individual.

So Mr. Sherman, is data that contains any persistent identifier truly anonymized?

*Mr. Sherman. Absolutely not. And I think this is the really key point, is that are there statistical privacy protecting techniques that are really important? Yes. But exactly to your point, when data brokers use the word "anonymized,'' it is a marketing term. It is not a technical term. And they use that to suggest that taking a name out of a data set somehow prevents it from being linked back to a person. And that is just not true. There is decades of computer science research showing the complete opposite.

And in fact, I would add that part of the whole business model of data brokers is aggregating and targeting people. The notion that they would not be able to do that or would not want to do that is just ridiculous.

*Mrs. Trahan. So that is exactly right. I mean, to follow up, would it not be a drafting mistake to treat personal data that is linked or can be linked to a persistent identifier as anonymized data?

I mean, if Congress passed such language, how would a data broker take advantage of that situation?

*Mr. Sherman. A broker could remove something superficially from data like a name, and perhaps keep something else in there that they can combine with other data to identify that person. So not violating the law, but rendering the protection effectively ineffective.

*Mrs. Trahan. Thank you. And that is exactly why we need to be so careful when we are crafting these laws, and why we have to ensure that ADPPA is as strong as it was in the last Congress, if not stronger.

Now, when we talk about data brokers, we have to contextualize this in the real harms and dangers that their over-collection presents. When a user taps a pop-up and consents to the use of geolocation data, or when they drive their car and geolocation data is transmitted to the auto manufacturer, that should not be an invitation to an opaque

chain of advertisers, individuals, and law enforcement to invade their private lives, hunt them down and, as we have already seen from cases over the past year, prosecutors jail them for seeking reproductive care. Data brokers enable that process, and giving consumers back control over their privacy and the ability to opt out of data broker collection is how we can immediately stop it.

But geolocation data is not a persistent identifier. It is a unique type of data that is over-collected, valuable to advertisers, and providers -- provides some of the most pervasive insights into our personal lives, as Congresswoman Lesko and others have raised today. So Dr. Moy, does the transfer, sale, and disclosure of geolocation data warrant additional scrutiny from Congress? And how could it be abused?

*Ms. Moy. Absolutely. And just to tie this to your anonymization question, even when location data has been wiped of a person's name, you know, I mean, there are very few people who were present both at Georgetown Law School and here in the Rayburn building today. So if you had that information about 10 people, you would know that one of them

was me. And if you added in my home address, then -- and found a location point near there, then you would absolutely just be able to re-identify that information. So supposedly anonymous information is usually not pseudonymous, and can be linked back to an individual.

I absolutely think that geolocation information should be protected with heightened protections. It can be used to learn not only about someone's specific whereabouts for the purpose of targeting them, but also sensitive information like where they worship, where their kids go to school, where they live and work, whose house they visit overnight, those types of things.

*Mrs. Trahan. Well, thank you. I would just like to say that I am grateful for your work at my alma mater, Georgetown. They would find me, too, both of us. Georgetown has established itself as a leader in all things tech policy, and your expertise is a big reason why. So thank you for being here today.

*Ms. Moy. Thank you.

*Mrs. Trahan. I yield back.

*Mr. Griffith. The gentlelady yields back. I now

recognize the gentleman from Alabama, Mr. Palmer, for his five minutes of questioning.

*Mr. Palmer. Okay, I want to do this very quickly, because I have got a number of things I want to ask you.

The Fourth Amendment was mentioned -- obviously, the right of people to be secure in their persons, houses, papers, and effects.

The Supreme Court of the United States said that data brokers can be sued if they provide incorrect information. What I would like to know is can they be sued if they misuse accurate information, Professor Moy? And I mean like if they sold it to scammers, as has been mentioned.

*Ms. Moy. So --

*Mr. Palmer. Could you make it really quick, because --

*Ms. Moy. They -- yes, they -- under the Federal Trade Commission section 5, in theory, yes, cases could be brought against --

*Mr. Palmer. Could they be sued if individuals made it clear that they didn't want their information sold? Should that be a requirement on any transaction that says -- where you can say, "I do not want my information to be shared or

sold or transmitted to any other party''?

*Ms. Moy. I believe so, yes.

*Mr. Palmer. Should that be part of our legislation?

*Ms. Moy. Yes, and I think the default should be don't share unless people agree in most cases.

*Mr. Palmer. Right, yes. It should be a positive decision, not negative.

Okay. The other thing is does the Fourth Amendment protections apply to sharing data with foreign governments? Because the Fourth Amendment protections that have been applied to data brokers has prohibited them from sharing information with the U.S. Government, although that is happening through certain Federal agencies.

*Ms. Moy. Yes. I mean, so the Fourth Amendment potentially does not protect against the sale of information to the U.S. Government or to foreign entities, either.

*Mr. Palmer. Okay. And that is another thing that needs to be in our legislation.

The foreign use -- I am -- one of the things I am very concerned about is the foreign use of data that they are purchasing for a number of things. One is

counterintelligence, because they can use this in -- to inform themselves on counterintelligence operations, where they can target people they have identified as key individuals.

We should not be allowing any of this information to be shared with, I think, any foreign entity, because you do not know whether or not it would be in the hands of adversarial -- whether they are adversarial nation states or actors, and then for propaganda purposes. And this is one of the things that concerns me right now is how so much misinformation is out there on social media, and they are targeting people that, you know, maybe that have conspiratorial leanings. And I think that this is becoming an issue, you know, micro-targeting election-type messages.

The other thing I want to talk about is, you know, the European Union has the general data protection regulation. Has this been effective? And any one of you who know anything about this can -- has this been effective for protecting personal data for people in the EU?

*Mr. Erwin. Yes. I mean there are a few things that GDPR did right.

*Mr. Palmer. Make it really quick, because --

*Mr. Erwin. It has not been as effective as --

*Mr. Palmer. That is what --

*Mr. Erwin. -- would have liked.

*Mr. Palmer. -- find out. Thank you.

And what about California's Consumer Privacy Act? Because it does open up opportunities for civil litigation, I believe.

*Ms. Moy. I think that it is making an impact. Certainly, the privacy officer is making an impact, as is the rulemaking authority that is given to it.

*Mr. Palmer. Okay. I would like your -- and maybe -- I had to step out to go speak to a group -- I would like for you to provide some information in terms of how we can work to get information that is already out there removed.

And again, my concern is the privacy protections that companies offer. But there are companies out there that will -- that you can pay to try to remove your information. But there are so many of these places where this information is, they could remove it from 500 and it would still be innumerable places where your information is still available,

and some -- whether they are legal or illegal.

How would you recommend that we go about crafting a bill to allow people to, as definitively as possible, get their information removed?

*Ms. Moy. So I do think that a lot of the information just shouldn't be out there in the first place, right? I mean, like, the fact that so many entities, hundreds, potentially thousands, may have some of the same data points, thousands of data points about each individual, that should not be the case. We should not have to opt out of those brokers having our information.

But, you know, in the event that they do, it should be very, very simple for a person to opt out everywhere, or it should only be collected on an opt-in basis.

*Mr. Palmer. I thank the chairman. I -- this is another example this week of a bipartisan hearing that I think has been very valuable, and I really appreciate the witnesses' time and your responses to allow me to get all these things in. So, Mr. Chairman, I yield back.

*Mr. Griffith. The gentleman yields back, and I appreciate that, and now recognize the gentlelady from

Florida, Mrs. Cammack, for her five minutes.

*Mrs. Cammack. Thank you, Mr. Chairman. Thank you to our witnesses for hanging in there with us. It is one of those crazy days where we are all in and out. So I appreciate you all.

I may have missed some of this, so if this is repetitive, I apologize. But in your estimation -- and I am going to direct this to you, Mr. Erwin -- in your estimation, what percentage of Internet users are using Web browsers that are privacy invasive?

*Mr. Erwin. Probably more than half the market. And by privacy invasive, I would take that to mean they don't have the baseline set of privacy protections --

*Mrs. Cammack. Right.

*Mr. Erwin. -- that protect them from cross-site tracking, cookie tracking, those type of protections.

*Mrs. Cammack. Don't worry, I won't ask you to name your competitors. I think we can draw our own assumptions on that. But more than half, it is pretty terrifying.

What kind of pushback have you and your company received from website advertisers or users as your company has

implemented tools that block cross-site tracking?

For example, do they have a worse ad experience? Is the algorithm tweaked to downplay impressions?

*Mr. Erwin. Yes, I think when we launched the initial version of our protections in 2019 we heard that users were not going to like it. And many what we call ad tech companies pushed back and essentially said the sky is going to fall. And, you know, our consumers generally are positive. This has not degraded their experience at all. Rather, they have a better experience in Firefox, because we are blocking this tracking.

The feedback we have gotten from ad tech providers, from advertisers, is not as positive, which is something that we would expect. And, you know, sometimes it is a positive thing when we hear negative feedback back like that. So --

*Mrs. Cammack. Did you guys take a hit in terms of revenue generation from advertising?

*Mr. Erwin. We -- it probably negatively impacted our revenue, but not by a significant degree.

*Mrs. Cammack. Okay. Thank you for that. And I may have missed it, but there may have been a conversation today

had about the possibility of a data brokerage that is in line with compensating users and consumers for their data with their consent to be -- to sell their data. I don't know if that has been discussed today, but I would love to get your feedback on how something like that might happen.

If a consumer consented to having their data sold, how would we go about compensating them for doing that? I am not talking about a class action suit or anything, but a marketplace system where we could do that. You look very eager to answer that question, Mr. Sherman.

*Mr. Sherman. I think the challenge with that here is that when we talk about data brokers, we are not talking about that first-party app or website necessarily you are giving it to to use the data for a business purpose. We are talking about that company selling it to third parties, we are talking about third parties consumers often don't know exist that are selling it for profit.

And so often times -- most of the time, I would say -- this is done with no consent whatsoever from the consumer.

*Mrs. Cammack. Absolutely, right. And I think we all acknowledge that most of the data that is sold today, it is

done without their consent. I mean, there is that veil of you consent to the terms and services of this app, whatever, and therefore we do what we will with your data that we collect and sell.

But shouldn't there be a way in which consumers can then earn a commission or something off of that, or something as simple as being notified when their data has been sold?

*Mr. Sherman. I think consumers should be made aware of this practice. Again, I think, you know, companies will -- an app or something will throw out these insanely long privacy policies that nobody actually reads, and then say that is consent.

I still think we need to prohibit the sale of some kinds of data, but I agree with what you said, that those terms should be made easy to read. It should take a few minutes maybe to scan through and see what kinds of data is this app collecting, is it sharing it or selling it with any third parties. That way the consumer has that information.

*Mrs. Cammack. Absolutely. And I want to yield the remainder of my time to my colleague from the great state of North Dakota. Thank you.

*Mr. Armstrong. I just have one more -- well, I have one minute, so I am going to be very quick.

Section 101 of the ADPPA prohibits the collection, processing, or transfer of covered data to what is necessary and proportionate to provide the specific product or service requested by the individual or permissible purpose. "Permissible purpose'' includes collecting, processing, or transferring data to prevent, detect, protect against, or respond to illegal activity, which is defined as a violation of a criminal law that can directly harm.

And my question for you, Ms. Moy, is I like the idea of this, and I don't know if you can answer it in 25 -- 28 seconds. Actually, I know you can't. But do we need to tighten this up a little better?

*Ms. Moy. I do think that -- yes. I mean, I think that this carve-out is in a bunch of privacy laws, kind of like the idea that for the detection -- or for the detection of fraud, or for the investigation of crimes, that there is an exception there. And I think in general that those exceptions should be tightened up, yes.

*Mr. Armstrong. Thank you.

*Mr. Griffith. The gentleman yields back to the gentlelady, and the gentlelady yields back to the chair.

*Mrs. Cammack. That is right, I do.

[Laughter.]

*Mr. Griffith. And I don't see any additional members wishing to ask questions. Seeing there are no further members -- who have time they haven't already used.

[Laughter.]

*Mr. Griffith. Seeing there are no further members wishing to ask questions, I would like to thank our witnesses again for being here today.

I will tell you I think this has been a very important hearing. I hope that C-SPAN will run it, so the public is more aware of what is going on, particularly if they run it in prime time, but you never know what they are going to pick and choose to run. It might be a month from now it will pop up.

That being said, in pursuance to committee rules, I remind members that they have 10 business days to submit additional questions -- that would be you, Mr. Armstrong -- for the record, and I ask that witnesses submit their

response within 10 business days upon receipt of the questions.

Without objection, the committee is adjourned.

[Whereupon, at 4:00 p.m., the subcommittee was adjourned.]