

STRENGTHENING DATA SECURITY TO PROTECT CONSUMERS

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION,
PRODUCT SAFETY, AND DATA SECURITY

OF THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MAY 8, 2024

Printed for the use of the Committee on Commerce, Science, and Transportation



Available online: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

61–851 PDF

WASHINGTON : 2025

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota	TED CRUZ, Texas, <i>Ranking</i>
BRIAN SCHATZ, Hawaii	JOHN THUNE, South Dakota
EDWARD MARKEY, Massachusetts	ROGER WICKER, Mississippi
GARY PETERS, Michigan	DEB FISCHER, Nebraska
TAMMY BALDWIN, Wisconsin	JERRY MORAN, Kansas
TAMMY DUCKWORTH, Illinois	DAN SULLIVAN, Alaska
JON TESTER, Montana	MARSHA BLACKBURN, Tennessee
KYRSTEN SINEMA, Arizona	TODD YOUNG, Indiana
JACKY ROSEN, Nevada	TED BUDD, North Carolina
BEN RAY LUJAN, New Mexico	ERIC SCHMITT, Missouri
JOHN HICKENLOOPER, Colorado	J. D. VANCE, Ohio
RAPHAEL WARNOCK, Georgia	SHELLEY MOORE CAPITO, West Virginia
PETER WELCH, Vermont	CYNTHIA LUMMIS, Wyoming

LILA HARPER HELMS, *Staff Director*

MELISSA PORTER, *Deputy Staff Director*

JONATHAN HALE, *General Counsel*

BRAD GRANTZ, *Republican Staff Director*

NICOLE CHRISTUS, *Republican Deputy Staff Director*

LIAM MCKENNA, *General Counsel*

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY,
AND DATA SECURITY

JOHN HICKENLOOPER, Colorado, <i>Chair</i>	MARSHA BLACKBURN, Tennessee, <i>Ranking</i>
AMY KLOBUCHAR, Minnesota	DEB FISCHER, Nebraska
BRIAN SCHATZ, Hawaii	JERRY MORAN, Kansas
EDWARD MARKEY, Massachusetts	DAN SULLIVAN, Alaska
TAMMY BALDWIN, Wisconsin	TODD YOUNG, Indiana
TAMMY DUCKWORTH, Illinois	TED BUDD, North Carolina
BEN RAY LUJAN, New Mexico	CYNTHIA LUMMIS, Wyoming
PETER WELCH, Vermont	

CONTENTS

Hearing held on May 8, 2024	Page 1
Statement of Senator Hickenlooper	1
Statement of Senator Blackburn	3
Statement of Senator Welch	35
Statement of Senator Klobuchar	37
Statement of Senator Budd	41

WITNESSES

James Everett Lee, Chief Operating Officer, Identity Theft Resource Center (ITRC)	4
Prepared statement	6
Sam Kaplan, Senior Director and Assistant General Counsel, Public Policy and Government Affairs, Palo Alto Networks	13
Prepared statement	14
Prem Trivedi, Policy Director, New America's Open Technology Institute	18
Prepared statement	20
Jake Parker, Senior Director of Government Relations, Security Industry Association	25
Prepared statement	27

APPENDIX

Letter dated May 7, 2024 to Hon. Maria Cantwell, Hon. Ted Cruz, Hon. John Hickenlooper and Hon. Marsha Blackburn from Main Street Privacy Coalition (MSPC)	47
Letter dated May 8, 2024 to Hon. Maria Cantwell and Hon. Ted Cruz from Karen R. Harned, Executive Director, Citizens for Legal Reform	51
Letter dated May 9, 2024 to Hon. John Hickenlooper and Hon. Marsha Blackburn from Jordan Crenshaw, Senior Vice President, U.S. Chamber of Commerce	53
Response to written questions submitted to James E. Lee by:	
Hon. Maria Cantwell	57
Hon. Ben Ray Lujan	59
Response to written questions submitted to Sam Kaplan by:	
Hon. Maria Cantwell	60
Hon. Ben Ray Lujan	62
Response to written questions submitted to Prem Trivedi by:	
Hon. Maria Cantwell	63
Hon. Ben Ray Lujan	64

STRENGTHENING DATA SECURITY TO PROTECT CONSUMERS

WEDNESDAY, MAY 8, 2024

U.S. SENATE,
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT
SAFETY, AND DATA SECURITY,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m., in room SR-253, Russell Senate Office Building. Hon. John Hickenlooper, Chairman of the Subcommittee, presiding.

Present: Senators Hickenlooper [presiding], Klobuchar, Schatz, Markey, Baldwin, Duckworth, Luján, Welch, Blackburn, Fischer, Moran, Sullivan, Young, Budd, and Lummis.

OPENING STATEMENT OF HON. JOHN HICKENLOOPER, U.S. SENATOR FROM COLORADO

Senator HICKENLOOPER. Welcome to Subcommittee on Consumer Protection, Product Safety, and Data Security. We'll come to order. I apologize for a little bit of the wait, and we'll—Senator Blackburn will be here quickly. She's en route.

We're at a pivotal moment in the age of technologies that rely on increasing amounts of consumer data. Obviously, if artificial intelligence has gotten the lion's share of publicity, but that's nowhere near the limit. Businesses collect or process data ranging from personally identifiable information, name, address; likeness, they say, in college these days; obviously sensitive data, physical locations, browsing history.

The threats to consumers' data that companies face is complex and in almost every way daunting. As companies collect more data, they become more attractive targets for data breaches. And by that, I mean criminal activity. Each breach costs companies nearly \$4.2 million per incident, and consumers shoulder the financial burden and the reputational harm of each incident.

How many more consumers need to be victims of identity theft for us to take action? How much longer should we allow personal data to be sold on the dark web for profit? When will cybercriminals be stopped, or at least deterred from preying on our data?

These data breaches hope—hurt small businesses, large corporations, and everything in between.

In 2023 alone, there were 3,205 data breaches in the U.S. That's what we know of, that were reported.

353,000 individuals were severely impacted.

Ten percent of publicly traded companies reported a data breach, impacting, in total, 143 million individuals.

These data breaches could have devastating effects. Nationwide, wireless carriers' data breach exposed the data of 70 million customers.

A large health insurer—this was recently widely reported—saw their system grind to a halt, which delayed important health care payments and exposed critical health data.

This is why we need strong requirements for how companies collect and protect our data by conducting routine risk assessments and establishing strong internal and external safeguards for data.

We need a strong national privacy standard that includes data minimization and data security. Obviously, data minimization establishes specific categories to—to turn off the spigot, as it were—to turn off the spigot of data so the companies collect—that the companies collect from consumers, so the companies aren't just collecting everything they can.

Data security establishes clear requirements for how companies should safeguard the data that they do collect, so breaches are less common.

We need to give consumers meaningful control over how their data is used. This will restore consumers' confidence in the technology that powers our economy. And I think states clearly are not waiting for the Federal Government to act. Already, 16 states, including Colorado, have passed or are in the process of passing their own state privacy laws. Other states are talking about it.

There are lessons we can learn from these state laws. For example, Colorado's law has a temporary right to cure for businesses to comply or adapt to privacy requirements.

There are also areas where the Federal Government has to step in to issue rules and apply enforcement, consistent definitions for key terms like sensitive data, or to issue nationwide rules.

The draft American Privacy Rights Act is an important bipartisan compromise framework for Congress to build upon. I commend Chair Cantwell and Chair McMorris Rodgers in the House for their efforts to bring this proposal forward.

We're committed here to listening to all perspectives on data minimization and data security. Minimization and security are obviously interconnected, interrelated. Together, they represent the foundation of a strong data privacy framework upon which we can build.

We have an opportunity right now and an obligation right now to build meaningful bipartisan consensus around these complex issues. That's why I look forward to the hearing today with each of our witnesses. I'd like to welcome each of our witnesses who are joining us today: James Lee, Chief Operating Officer from Identity Theft Resource Center; Sam Kaplan, who's the Assistant General Counsel of Palo Alto Networks; Prem Trivedi, Policy Director for New America's Open Technology Institute; and Jake Parker, Senior Director of Security Industry Association.

I now recognize our Ranking Member, our Vice Chair, Senator Blackburn, for her opening remarks.

**STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE**

Senator BLACKBURN. Thank you so much, Mr. Chairman, and welcome to each of you. And apologies for people kind of coming and going. We had a 230 vote that ended up getting called.

But I am so pleased. I know Chair Cantwell and Ranking Member Cruz are on the floor right now, but I am appreciative that Chair Cantwell has brought privacy back into focus.

And I've worked for over a decade for Congress to take an action in this area. And when Senator Welch and I were each on the House Energy and Commerce Committee, in 2012, we brought forward the Data Security and Breach Notification bill. It was the first of the privacy and data security bills, and it was bipartisan.

It would take steps to protect the security of data there from businesses. It would have required consumer data breach notifications, and allowed the FTC and state attorneys general to hold companies accountable for violations of the law. So that is where we were in 2012.

And as we now know, this issue, since it hasn't been addressed, and it hasn't been resolved, it is growing more and more urgent every single day for an action to be taken.

The need for the swift adoption of smart and effective data privacy and security legislation is pressing for several reasons.

First, China and other bad actors are not slowing down. Now FBI Director Christopher Wray was before us at a judiciary committee meeting, and he said something pretty significant. He said, "If you are an American adult, it is more likely than not that China has stolen your personal data." And he also said, "China's vast hacking program is the world's largest, and they have stolen more Americans' personal and business data than every other country combined."

We need to be paying attention to this. This threat is especially magnified as China seeks to become the world leader in artificial intelligence by the time we get to 2030. China plans for AI to power its vast surveillance state, and data collection and retention is at the heart of their strategy. At the same time, as AI technology becomes increasingly intertwined in our daily lives here in the U.S., consumers have valid questions about how their data is going to be used to train these large language models and AI applications.

I hope today that we will discuss why we need Federal privacy and security legislation to combat these threats.

Second, Congress is past the point where we risk ceding our authority to both states and other countries. As we all know, state governments are quickly enacting privacy laws, creating a patchwork of regulatory headaches for our businesses. Fifteen such laws exist, including Tennessee and Colorado.

And the Europeans have also beaten us to the punch. Several years ago, they did GDPR. They are now using GDPR as the foundation for regulating AI.

Yet, we can use the EU as something of a cautionary tale about the need to make our regulation smart and effective. I visited the EU to work on this issue last year, and I heard stories from one of their data protection authorities about how they've been asked

to resolve disputes over bank accounts after a couple divorced, or to resolve a dispute between neighbors about the location of an antenna.

So let's be smart, let's not make these same mistakes, and let's not overreach. We know our friends, the Europeans, always have a heavier-handed approach, which makes it even more imperative that we act in a thoughtful manner.

More, without congressional action, the FTC will proceed ahead with its Commercial Surveillance and Data Security rulemaking, which it launched in 2022 without congressional authority and directive. Congress should be setting these rules, not unelected bureaucrats.

Finally, while this hearing will likely feature much discussion on concepts like data minimization and other data security practices, we must not forget about the cybersecurity threats posed by new and emerging technologies.

One area of great interest to Tennessee are quantum technologies. Through methods like harvest now, decrypt later, once bad actors steal encrypted data today, nothing can stop them from decrypting your data tomorrow with quantum technology.

That is why this committee must move quickly to examine this technology and reauthorize the National Quantum Initiative Act.

I would love to work on this with our Chairwoman and the team here at the Committee. Tennessee is a leader in financial innovation in technologies like quantum computing, and the Oak Ridge National Lab is at the forefront of basic and applied science research. When I speak with people in the state, they ask me how we can best tackle privacy and data security issues, while also continuing to allow innovation to flourish.

This committee must be thoughtful in our approach, but also mindful of the realities the congressional calendar imposes.

I look forward to our discussion today, and I so appreciate the testimony from each of you.

Thank you, Mr. Chairman.

Senator HICKENLOOPER. Great. Now we'll hear the opening remarks from each of our witnesses. The term "witness" gives a false sense of, I don't know, insecurity, perhaps, these days. Anyway.

We'll start with James Lee, who's Chief Operating Officer, Identity Theft Resource Center.

STATEMENT OF JAMES EVERETT LEE, CHIEF OPERATING OFFICER, IDENTITY THEFT RESOURCE CENTER (ITRC)

Mr. LEE. Thank you, Mr. Chairman, Ranking Member Blackburn.

I am James Lee. I am the Chief Operating Officer of the Identity Theft Resource Center. I'll refer you to our full written remarks to find out more about the ITRC, but just so everybody knows, the core of our business is to provide free assistance to victims of identity crimes. And we also do research and analysis on identity crime trends, which we make available to both the public and private sector.

So a lot has happened since we were in this room back in 2021 to talk about this very same subject. We've seen bad actors shift

their focus. We've seen them expand their reach, and we've seen them accelerate their innovation attempts.

We may, in fact, be at the very beginning of what is a golden age of identity crime. It's fueled by stolen personal data, made highly effective and efficient by AI, with individuals and many businesses all but helpless to defend themselves.

So why do I say that? I'm going to give you some scope of the problem.

So data breaches are the fuel for identity crimes—all identity crimes—and a fair portion of cyberattacks, thanks to stolen login and passwords. In 2023, the total number of data compromises was 3,205, as the Chairman pointed out.

That impacted an estimated 353 million people, because some people were hit more than once. That's a 78 percent increase from the year before. That's a 72 percent increase from the previous high, which happened the last time we had this hearing.

From a financial standpoint, more than two-thirds of the people who contact the ITRC are losing more than \$500. Within that subset, 30 percent of them are losing more than \$10,000. And we are now routinely hearing from people who are losing six and seven figures in financial losses due to identity scams.

The most troubling trend, though, is the number of people who have decided that their only way out is self-harm. Sixteen percent of the people who contacted us in 2023 said they contemplated taking their own life. For the decades before that, that number had never been higher than two to four percent. And now 16 percent, doubled in one year, and we do not see it slowing down.

And also, unlike past years, we now hear routinely from grieving families who are still being attacked by the identity criminals who are trying to keep the scam going.

We don't advocate one way or the other for legislation or regulation for the most part, but we do provide objective information. So with that in mind, we're still at the same place we were last time.

The best way to help identity crime victims is to prevent victimization in the first place. And an important part of preventing identity crimes is through uniform minimum standards for data protection and use. Minimum technical and non-technical standards are essential in our world that's driven by software and fueled by data.

Compliance with comprehensive, but not necessarily prescriptive, minimum standards can reduce the risk of exploitation. Minimum standards are more than just metrics, though, which is what we tend to think of a lot of times.

They are practices like data minimization, which is a concept that is predicated on a very simple truth. If you do not have the data, you cannot lose it. And if it's secure, it cannot be misused. Until we get to quantum computing. And that's a different discussion.

Routine risk assessments also help ensure information systems are secured in a manner equal to the risk—that's very important—equal to the risk that an organization faces.

You add two other complementary concepts, privacy by design and security by default. And you have all the tools needed to keep privacy and security at the forefront of a company's culture and in every stage of a product's life.

To be effective in reducing identity crimes, uniform standards also need strong enforcement. Defenders must continually measure their progress and constantly adjust to the new tasks, and you do that through audits.

There's also the need for strong enforcement actions when it comes to data breach notices, which are increasingly ineffective, even if a notice is issued.

Let me give you two examples.

In the first three months of this year, 32 percent—32 percent of data breach notices had some information about what caused the data breach if it was linked to a cyberattack.

Reverse that number, and that tells you how many didn't include information about what happened. That number was 100 percent of data breach notices, until the fourth quarter of 2021.

The average number of new data breach notices in the U.S. is nine per day. In the European Union, one of the things they do get right, 335 every day.

We are missing data breach notices. And there are plenty of examples to prove that.

Let me leave you with one final thought. If we adopt data minimization, and we should, and if we give consumers more access and control over their personal information, that is a vital part of data protection. They can significantly reduce the amount of personal information at risk of a data breach and misuse by criminals.

But, because you knew there was going to be one. But, personal information used responsibly and transparently is important for proving a person is who they claim to be in a variety of transactions, from opening a bank account to applying for a government benefit, et cetera.

But they also effectively prevent someone from becoming a victim of identity fraud because of stolen personal information. Restricting the use of personal information for identity verification and fraud prevention as part of consumer control or data minimization could have the unintended effect of actually aiding identity criminals and negatively impacting communities that are already disproportionately affected by identity crimes.

So thank you for your time and attention. I look forward to answering your questions.

[The prepared statement of Mr. Lee follows:]

PREPARED STATEMENT OF JAMES EVERETT LEE, CHIEF OPERATING OFFICER,
IDENTITY THEFT RESOURCE CENTER (ITRC)

Introduction

Good afternoon, Chair Hickenlooper, Ranking Member Blackburn and members of the Subcommittee. Thank you for the honor of speaking with you today. My name is James Everett Lee and I am the Chief Operating Officer of the non-profit *Identity Theft Resource Center* (ITRC) based in San Diego, California.

For 25 years the ITRC has offered free assistance to victims of identity crimes. In that time, our contact center staffed by trauma-informed advisors has helped hundreds of thousands of victims recover their identities that have been stolen, misused, or otherwise compromised.

Through our website and outreach programs, we have helped millions of individuals avoid becoming identity crime victims by teaching them how to protect their information. We also provide information about the latest scams that involve the theft or misuse of personal information.

Since 2005, the ITRC has compiled the largest repository of publicly reported data breaches and other forms of identity data compromises. What started with a single

notice and a handful of data points nearly 20 years ago has grown into a database of more than 20,000 data breaches with as many as 96 data points per event that is updated daily.

The ITRC publishes an annual data breach report and quarterly updates that analyze the trends reflected in the data breach notices mandated by state law and Federal regulations. We make this information available for free to consumers in the form of a searchable database as well as a free alert service that informs them when an organization they enroll with the ITRC posts a data breach notice. A more robust version of the data and services are available to businesses, government agencies, and institutions for a nominal fee.

Today I'll touch on our findings related to the current trends in identity crimes based on first-hand reports from the new victims who reported more than 13,000 incidents to the ITRC in 2023. I will also touch on the impacts of identity crimes and cyberattacks on general consumers and small businesses. This information comes from our annual research reports which are attached to these remarks.

I will also reference two additional ITRC reports from 2023 that provide some context to the topic for today's hearing: Research of first impression on the impact of identity crimes in Black communities; and, a discussion paper on the challenges to verifying a person is who they claim to be in a time when key points of personal information has been compromised for most adults in the never-ending series of data breaches. These, too, are attached for your reference.

Finally, for the Subcommittee's awareness, the ITRC is a 501(c)3 non-profit funded primarily through grants from the U.S. Department of Justice, Office of Victims of Crime (DOJ-OVC) as well as private contributions, corporate sponsorships, and donations. We work closely with key Federal agencies on issues that involve identity crime victims including the Federal Trade Commission (FTC), the Internal Revenue Service (IRS), the Department of Treasury (Treasury), the Federal Reserve, the Pandemic Response Accountability Committee (PRAC), and the Department of Homeland Security (DHS). We provide data breach information to many of these same agencies. We also offer online, Live Chat access to ITRC Advisors to state and local law enforcement agencies and other non-profit organizations under a DOJ grant. A full list of our financial supporters and partner organizations is available on our *website*.

The Golden Age of Identity Crime

A lot has transpired since the last time the ITRC was part of a full committee hearing on a similar topic in October 2021. On that day we coincidentally published a quarterly data breach report that showed we had already passed the total number of compromises recorded in 2020 and were only 238 data events away from tying the all-time record set in 2017. In fact, we did set a record for publicly reported data breaches later in 2021—1,860.

We were still struggling at that time to understand the scope and scale of the identity fraud committed during the pandemic when identity criminals were able to use information stolen in data breaches to impersonate unwitting victims. That information was, and still is, used to open bank accounts, obtain loans, and trick innocent, trusting people into willingly sharing personal information with someone they thought they knew—often on a social media platform or as part of a romance scam.

Given the ITRC's role as a victim advocacy organization, we offered a singular prescription: To reduce the number of identity crime victims—and crimes—reduce the number of data breaches linked to cyberattacks. To do that, we discussed three needs:

- The need for better cybersecurity and data protection standards and practices
- The need for better enforcement of cybersecurity and data protection regulations
- The need to fix the data breach notice system

Fast forward to today and the needs are still the same. What has changed is the urgency required to address those needs along with the opportunity to devalue personal information stolen by identity criminals.

Since 2021, we've seen bad actors shift tactics, expand their reach, and accelerate the pace of innovation. The results of these actions are the highest number of data breaches we've ever seen, often with devastating financial and emotional impacts on the individuals caught in the crossfire between professional identity criminals and the business or data source they target.

Add to the mix the introduction of generative artificial intelligence, and you have a recipe for a prolonged period of identity crime—fueled by stolen personal data, made highly effective and efficient by AI, with individuals and many businesses all

but helpless to defend themselves. What we now have is all the ingredients for a Golden Age of Identity Crime.

Today's Trends

Today's trend lines support the classic definition of a Golden Age: great wealth, growth, innovation, and a kind of stability that supports long-term achievement.

Beginning with data breaches—the fuel for virtually all identity crimes and a fair portion of cyberattacks. The number of data compromises reported in the United States surpassed two significant milestones in 2023: The highest number of data events reported in a single year and exceeding 2,000 (and ultimately 3,000) events in a single year.

The total number of data compromises reached 3,205, impacting an estimated 353 million victims, including those affected by multiple compromises. The 2023 compromises represent a 78-percentage point increase over the previous year and a 72-percentage point hike from the previous all-time high number of compromises set in 2021.

Total Compromises by Year		
	Compromises	Victims
2023	3,205	353,027,892
2022	1,801	425,212,090
2021	1,860	300,607,163
2020	1,108	310,235,204
2019	1,279	883,558,186
2018	1,175	2,227,849,622

SOURCE: ITRC 2023 Data Breach Report, January, 2024

As of May 6, 2024, we have recorded 1,178 data breaches impacting an estimated 64 million people in 2024. Historically, Q1 is the lowest point in each year in terms of data breach notices, so we are already on a path for another record-setting year.

The steady downward drift in terms of the estimated number of individual victims may appear to be a positive trend, but is in fact an illusion. The number of victims impacted in 2023 represents a 16-percentage point reduction from 2022 when more than half of the total annual victim count was related to three breaches announced late in the previous year. By any measure, there are simply too many victims.

A single or series of small events can also rapidly reverse a downward victim trend. Through Q1 2024, the number of victims reported by compromised organizations dropped 81 percent (81 percent) from the last Quarter of 2023. However, a series of breaches in April this year has already more than doubled the victim count for the year.

That number does not include the ransomware-related breach at United Healthcare's Change subsidiary which will significantly increase the number of victims. Based on company comments, the number of victims could exceed one-third of U.S. residents given United Healthcare's market share. To date, United Healthcare has not offered a specific victim estimate.

United Healthcare aside, the decline in the number of individual victims is largely attributed to the fact that organized cyber and identity criminals do not need to acquire personal and business information on the scale they once did. The kinds of attacks that lead to data breaches today are more targeted in terms of the organization that is attacked, the information sought, and the goal of the attack (financial or intelligence). The result is more attacks against a broader set of businesses, but a smaller footprint in terms of individual victims in any single attack. For example, in Q1 2024 attacks increased in 15 of 17 industries year over year, but the overall victim count decreased.

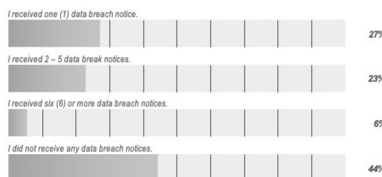
	Year					
	Q1 2024		Q1 2023		Q1 2022	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	36	501,925	31	569,618	21	106,099
Financial Services	224	18,262,986	70	10,555,103	68	5,732,597
Government	43	126,500	23	759,622	13	790,763
Healthcare	124	6,071,259	81	14,199,413	73	4,377,462
Hospitality	16	687,334	7	196,891	6	57,392
HR/Staffing	4	119,758	3	20,616	-	-
Manufacturing	77	143,423	49	1,190,146	52	249,706
Mining/Construction	19	10,032	15	59,292	-	-
Non-Profit/NGO	38	824,029	19	85,420	20	629,822
Professional Services	100	683,246	48	75,502	45	3,022,491
Retail	22	39,092	16	179,622	18	272,950
Social Services	1	5	3	154,160	-	-
Technology	40	634,212	35	24,399,696	16	10,832,588
Transportation	38	122,942	13	11,096,783	8	20,930
Utilities	18	204,730	6	37,054,637	-	-
Wholesale Trade	11	10,690	11	62,316	-	-
Other	28	154,727	12	27,698	64	675,411
Unknown	2	2	-	-	-	-
Totals:	841	28,596,892	442	100,686,535	404	26,768,211

SOURCE: ITRC Q1 2024 Data Breach Analysis, April 2024

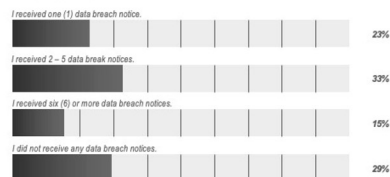
The trend of fewer individuals being impacted is somewhat offset by the fact individuals were likely to be the victim of multiple data breaches in 2023. Breach victims are also more likely to be the victims of identity misuse.

Have you received data breach notices in the past 12 months?

GENERAL CONSUMERS



ITRC VICTIMS

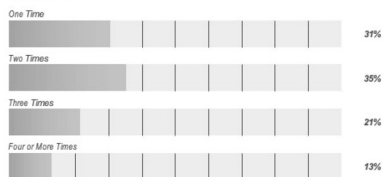


SOURCE: ITRC Consumer Impact Report, August 2023

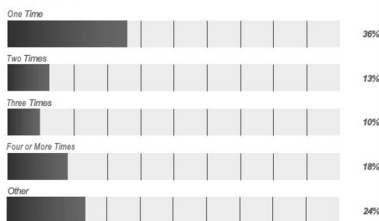
In fact, there is a general victim impact trend where more individuals are reporting multiple instances of identity misuse as part of a single event in addition to being victimized multiple times. In 2021, 29 percent of victims who contacted the ITRC reported being the victim of previous identity misuse. By 2023 that number was 41 percent. The number is even higher among the general population who do not contact the ITRC for help—69 percent (69 percent):

How many times have you been the victim of an identity crime (not including data breaches)?

GENERAL CONSUMERS



ITRC VICTIMS



SOURCE: ITRC Consumer Impact Report, August 2023

From a financial standpoint, in 2021 only nine percent (9 percent) of victims of identity crimes lost more than \$10,000, with 35 percent of victims losing less than \$500. Today, nearly two-thirds of victims report losing more than \$500 with 30 percent (30 percent) reporting losses of \$10,000 or more. For the first time in the ITRC's 25-year history, we now routinely receive reports of six and seven-figure losses due to identity-related scams.

The most troubling trend, though, is the dramatic rise in the number of individuals who contemplate self-harm as a result of being the victim of an identity crime. When we discussed the wide range of identity crime impacts during the 2021 committee hearing, the number of victims who contemplated suicide had jumped from a 20-year norm of two to four percent (2–4 percent) to eight percent (8 percent) during the pandemic.

Today that number stands at 16 percent (16 percent) with no sign of slowing. And, unlike past years, we now regularly receive phone calls from grieving family members whose loved one took their own life—and are still being attacked by the same identity criminals seeking to keep the scam alive. From fake go-fund-me campaigns to raise money for funeral expenses to continuing to post from the deceased person's social media account to draw other people into the scam, victims are losing their life savings and their lives at the hands of identity criminals. Here's an *example*. [<https://www.thedailybeast.com/feds-say-sick-celebrity-romance-scam-led-to-retired-teachers-suicide>]

All of these impacts bring us back to the topic at hand: Can we reduce the number of identity crimes and crime victims with better cybersecurity and data protections?

The short answer is yes.

First, let me make it clear that the ITRC does not advocate for or against any particular legislation or regulation. We do, however, provide objective information on the underlying issues prompting a proposed or active policy. With that in mind, the ITRC continues to believe that the best way to help identity crime victims is to prevent victimization in the first place.

And, the best way to prevent victimization is to prevent the loss of personal information in data breaches in conjunction with making stolen personal information less valuable to criminals. To do that we still believe we need:

- Minimum cybersecurity and data protection standards, including regular risk assessments
- Enforcement of cybersecurity and data protection laws and regulations backed by audits
- A new way of addressing data breach notices

And I'll add a fourth item: Protect the appropriate uses of information and enhance anti-fraud and identity verification with the responsible use of biometrics to devalue stolen personal information.

Let me take these one by one:

Having uniform minimum standards for data security and protection that can be routinely measured is the price of entry to a world where software is part of every aspect of our lives. Our cars are computers on wheels. Our phones aren't just used for talking. The toothbrush I just bought is software-driven and I paid for it with a credit card that has a chip in it.

We've seen the tragic results of poor software in the aviation industry, and we know the risks if a rogue actor or Nation/State exploits critical infrastructure.

It's not just software that runs things that benefits from minimum standards and data protection practices. So can the information that makes up each and every person's identity today.

In 2019, the ITRC did not track a single data breach attributed to a Zero Day¹ software flaw. By 2021, there were 4; in 2022 there were 8. In 2023 there were more than 100 data breaches caused by a bad actor exploiting a software bug the developer or security professionals did not know existed. Once considered rare, advanced tech like AI is making Zero Day attacks easy to plan and execute.

Once a software flaw is known, it can take months to apply a patch to enterprise software to operate every aspect of businesses. The larger the company, the longer it takes to patch a known flaw, all the while hoping a bad actor does not discover an unpatched bug.

The ITRC and other security researchers have all identified a steep rise in data breaches from unpatched software. If the worst-case scenario does occur and a flaw

¹A Zero Day software vulnerability is one that is discovered after software has been released into production. The term is commonly associated with cyberattacks.

is exploited, security teams likely won't know about the attack until it's been underway for an average of 204 days, according to IBM. It will still take another 73 days to contain the attack.

With the advent of AI, defenders have the tools to help find bugs and resolve attacks faster. But technology is agnostic—users are not. Bad actors also have tools to help find and exploit the inevitable bugs that make their way into production versions of software. Just last month (April 2024), the *University of Illinois* announced a discovery that allows generative AI to develop malware to take advantage of a software flaw just by reading the public alert used to notify software users of the vulnerability.

Minimum standards may also help reduce the number of so-called Supply Chain Attacks against third-party organizations that store or have access to the data of customers or partners. These smaller organizations tend to have fewer security resources and protections, but access to personal information from large and/or multiple entities.

From an identity criminal's perspective, a supply chain is Nirvana. Why risk getting caught or expend the time and energy to attack a large, well-defended organization when you can attack a vendor with fewer protections and the data of hundreds of organizations?

In the most recent ITRC data breach report from January 2024, we noted a steady increase in Supply Chain attacks over time.

Since 2020, the number of organizations impacted has surged by nearly 300 percent (300 percent)

Supply Chain Attacks by Year		
	Third-Party/ Supply Chain Attacks	Entities Impacted
2023	242	2,769
2022	115	1,745
2021	84	521
2020	69	694

SOURCE: ITRC 2023 Data Breach Report, January 2024

The chart illustrating the growth in Supply Chain Attacks includes organizations impacted by one of the largest third-party vendor attacks ever—a 2023 attack against the company that offers the MOVEit file transfer software and service. Cybercriminals exploited previously unknown flaws in software and cloud versions of MOVEit used by businesses, governments, schools, hospitals and other organizations around the world to securely share documents and information.

In Q1 2024, the number of organizations impacted by Supply Chain Attacks more than tripled compared to the same period in 2023. Fifty (50) new attacks in the Quarter impacted 243 organizations compared to 73 entities in Q1 in the previous year.

The United Healthcare/Change data breach will most likely turn out to be the largest Supply Chain attack we've ever seen just due to the sheer number of organizations in the Change supply chain and the number of individuals served by them.

These are examples of what happens when we do not have uniform, minimum standard for collecting, processing, and storing personal information. The recent discussion draft of the proposed American Privacy Rights Act (APRA) includes concepts already in place around the world and in some state laws and regulations. In particular, data minimization, risk assessments and routine audits to ensure organizations are continually adapting to ever-changing risks.

Data minimization is predicated on a simple truth: you cannot lose control of information you don't have or haven't secured. The logic is not complicated. If you don't need the information to complete a business transaction, don't collect it. If you need it, delete it as soon as the transaction is completed unless you are required to keep it. If you must keep the information, make sure it is secure and encrypted.

Routine risk assessments help ensure information and systems are secured in a manner equal to the risk an organization faces. Add two other complementary con-

cepts—privacy by design and security by default—to help keep privacy and security at the forefront of every stage of the product lifecycle.

An organization that embraces these actions also has the foundation to build a company culture that ensures Security and Data Protections are not just departments, but integral parts of every team member's job.

This leads to the second and third points: To be effective in reducing identity crimes, uniform standards need strong enforcement backed by routine audits. Cybersecurity is a race between attackers and defenders. Defenders must continually measure their progress and constantly adjust to the new risks at hand. An audit becomes part of the roadmap for building the defenses needed to keep pace with aggressive attackers.

The need for strong enforcement actions also applies to data breach notices which are increasingly ineffective.

Today, data security regulations are limited, compliance is weak and enforcement is spotty. Whether there are consequences for non-compliance written into regulations or disciplinary actions taken by regulators depends almost exclusively on geography and/or industry.

There are fines in the healthcare industry because HIPAA includes the ability to assess penalties when cyberattacks or data breaches result in personal health information being exposed. The Securities and Exchange Commission can, and does, take enforcement actions for failing to adequately secure data and systems that have a material impact on investors. The Federal Communications Commission also has a set of enforceable cybersecurity and data protection regulations.

Individuals and groups of state attorneys general also litigate following major data breaches. A few states have also adopted separate health and biometric data protection laws.

There is ample evidence to support the conclusion that the vast majority of breaches may go unreported; there are few if any consequences for non-compliance; and, breach notices increasingly contain little to no help helpful information for victims and other organizations seeking to avoid a similar attack. For example:

- From 2018 until 2021, 100 percent (100 percent) of data breach notices tracked by the ITRC included information about the root cause of the attack and a majority also included the number of victims impacted. Since Q4 2021, that number has dropped to the point where in Q1 2024, only 32 percent (32 percent) of data breach notices linked to cyberattacks contained information about the cause of the attack.
- In late 2023, following an SEC investigation and litigation by state attorneys general, tech services provider Blackbaud admitted that client information of more than 13,000 organizations had been compromised, but only 604 data breach notices were tracked by the ITRC. (Blackbaud was also fined for making false statements about the type of information exposed in the data breach, for making misleading statements about when they knew the information to be false, and for failing to secure sensitive personal information which it had earlier denied).
- An average of nine (9) new data breach notices were issued each day in 2023 in the United States. In the European Union in 2023, the daily rate of new data breach notices was 335 due to the uniform requirements of the General Data Protection Regulation (GDPR).

I would offer one final thought. Adopting data minimization and giving consumers more access and control over their personal information for certain uses are vitally important parts of data protection. These practices can significantly reduce the amount of unnecessary personal information at risk of a data breach and misuse by criminals.

However, there are also important uses of personal information that help ensure identity information is only used by the true person who owns that identity. Personal information, used responsibly and transparently, is important for proving a person is who they claim to be in a wide variety of transactions—from opening bank accounts to applying for government benefits, as examples.

Restricting the use of personal information for identity verification and fraud prevention would have the unintended effect of aiding identity criminals and negatively impacting communities that already are disproportionately affected by identity crimes. A two-year study by the ITRC revealed the challenges facing Black communities that would be made worse if the tools needed to accurately identify a person were restricted.

Data enhanced with tools such as biometric verification (not recognition) have the potential to reduce the value of stolen identity information. That, in turn, would re-

duce the incentive for criminals to steal the information in the first place and render already stolen information useless in verification processes.

Thank you for your time and attention. I look forward to answering your questions.

Senator HICKENLOOPER. Thank you very much.

Now Mr. Sam Kaplan, who is the Assistant General Counsel of Palo Alto Networks and has spent a considerable amount of time in Colorado.

**STATEMENT OF SAM KAPLAN, SENIOR DIRECTOR
AND ASSISTANT GENERAL COUNSEL, PUBLIC POLICY
AND GOVERNMENT AFFAIRS, PALO ALTO NETWORKS**

Mr. KAPLAN. Thank you Senator. Chairman Hickenlooper, Ranking Member Blackburn, and distinguished members of the Committee, thank you for the opportunity to testify on how cybersecurity is a critical and foundational element of data security and consumer protection.

Again, my name is Sam Kaplan, and I'm Senior Director and Assistant General Counsel for Public Policy and Government Affairs at Palo Alto Networks.

I've spent the bulk of my career working at the intersection of cybersecurity, national security, and data privacy. Prior to joining the private sector, I was proud to serve in a number of positions across the Federal Government, to include as the DHS Chief Privacy Officer, served on the Privacy and Civil Liberties Oversight Board, and at the U.S. Department of Justice.

For those not familiar with Palo Alto Networks, we are an American-headquartered company founded in 2005 that has since become the leading cybersecurity company. We proudly provide cyber defense capabilities to enterprises around the world, supporting 95 of the Fortune 100, critical infrastructure of all shapes and sizes, the U.S. Federal Government, universities, educational institutions, and a wide range of state and local partners.

This means that we have a deep and broad visibility into the cyber threat landscape. We are committed to being a good cyber citizen and a trusted security partner with the Federal Government.

It's no secret that cyber-attacks cause real impact to our daily lives, from disruptions of public services like health care or emergency services, to compromises of American sensitive data.

With that backdrop, Palo Alto Network strongly believes that deploying cutting edge cybersecurity defenses is a necessary and effective enabler of data security and privacy. Bottom line, effective data security and data privacy requires cutting edge cybersecurity protections.

Organizations should be encouraged to protect data by implementing robust data and network security practices that can both help prevent incidents and data breaches before occurring in the first place, and mitigate the impact should an incident occur.

To stay ahead of this evolving threat landscape, cybersecurity professionals regularly leverage security data, which is the network telemetry, the ones and the zeros, the malware analysis, the IP addresses, the vulnerability enumeration, that we must ingest and analyze in real time to optimize cyber defenses.

To that end, we are heartened to see cybersecurity generally included in privacy frameworks as a permitted purpose that companies like ours can use to collect, process, retain, and transfer security data, to in turn better protect those systems and data from compromise. Today's cyber threat landscape requires that approach, and everyone's personal privacy will benefit from that framing.

To that end, Palo Alto Networks recommends organizations focus on the following actions to bolster their cyber resilience, and increase their data security posture.

First, leverage the power of AI and automation. For too long, cyber defenders have been inundated with alerts to triage manually, which can lead to data breaches. AI can help flip this paradigm.

Second, ensure complete visibility of attack surfaces, to help identify and mitigate vulnerabilities before they can be exploited.

Third, implement a zero trust network architecture to prevent and limit an attacker from moving laterally across the network.

Fourth, promote secure AI by design, to assist with inventorying AI usage, applying policy controls, and securing applications built with artificial intelligence.

Fifth, protect cloud infrastructure and applications. As cloud adoption accelerates, cloud security cannot be an afterthought.

Sixth, maintain and test an incident response plan to prepare for and respond to cyber incidents.

Our team at Palo Alto Networks is dedicated to securing our digital way of life. We enthusiastically participate in a number of forums like CISA's JCDC, and share our situational awareness and understanding of the threat landscape with those key partners.

Our collaboration in forums like these reinforces that cybersecurity is truly a team sport.

Thank you again for the opportunity to testify on how cybersecurity is a foundational requirement of data privacy, and I look forward to your questions.

[The prepared statement of Mr. Kaplan follows:]

PREPARED STATEMENT OF SAM KAPLAN, SENIOR DIRECTOR AND ASSISTANT GENERAL COUNSEL, PUBLIC POLICY AND GOVERNMENT AFFAIRS, PALO ALTO NETWORKS

Chairman Hickenlooper, Ranking Member Blackburn, and distinguished members of the committee:

Thank you for the opportunity to testify on the importance of data security. Your committee's interest in better understanding cybersecurity's foundational role in enabling data privacy is greatly appreciated. My name is Sam Kaplan, and I am the Senior Director and Assistant General Counsel, Public Policy & Government Affairs at Palo Alto Networks. I've spent the bulk of my career working at the intersection of cybersecurity, national security, and data privacy. On behalf of my company, I offer our commitment to work in partnership with you and your staffs as you continue to examine this important area of public policy.

For those not familiar with Palo Alto Networks, we were founded in 2005 and have since become the global cybersecurity leader—protecting businesses, people, and governments across more than 150 countries. We support 95 of the Fortune 100, critical infrastructure operators of all shapes and sizes, the U.S. Federal government, universities, educational institutions, and a wide range of state and local partners.

Practically speaking, this means we have a unique vantage point into the cyber threat landscape. This information, paired with the insights we develop from helping organizations respond on a daily basis to complex cybersecurity incidents, puts

us on the front lines of the cyber defense battle. We are committed to using this mantle to be good cyber citizens and trusted security partners.

Cybersecurity Enables Data Privacy

Palo Alto Networks strongly believes that deploying cutting-edge cybersecurity defenses is a necessary enabler of data privacy. Organizations should be encouraged to protect data by implementing robust data and network security practices that both can help prevent cyber incidents and data breaches from occurring in the first place, and mitigate the impact should an incident occur.

Palo Alto Networks supports efforts to develop a strong Federal privacy standard that:

1. Provides consistent and predictable requirements and protections for individuals and businesses;
2. Establishes a single national standard to prevent a complex compliance patchwork;
3. Promotes robust and adaptable data security standards, spanning prevention to response, commensurate with today's evolving cyber threat environment;
4. Fosters innovation by recognizing the importance of automation in data security;
5. Prevents disclosure and transparency requirements from unintentionally creating roadmaps for threat actors to break through data and network defenses; and
6. Recognizes the beneficial uses of security data for permitted purposes, such as cybersecurity.

To keep pace with and respond to the increasingly sophisticated threat landscape, the cybersecurity community regularly leverages security data, through which cyber threat information is synthesized to develop a holistic picture of the techniques, tactics, infrastructure, and motives of cyber adversaries. Security data is the network telemetry—the 1s and 0s, the malware analysis, the IP addresses, the vulnerability enumeration—that we ingest and analyze to help defenders stay ahead of attackers.

The necessity of cybersecurity firms collecting, processing, retaining, and transferring security data cannot be stressed enough. As explained further below, automated cyber defense tools are already proving transformational for network defenders. Security data—across the network, endpoint, and cloud—is now enhanced, stitched together, and correlated in real-time to differentiate the threat signal from the noise. This, in turn, results in better fortified systems and enhanced data security.

To that end, recent policy approaches recognizing the importance of leveraging security data to bolster cyber defense is a positive development and one that will meaningfully help protect data privacy. Palo Alto Networks appreciates the growing recognition of this critical point, and believes that data privacy legislation should ensure that access to information for cyber defense purposes is not undermined by requirements intended to address other uses of consumer data.

Any Federal privacy law must ensure that cyber defenders can leverage security data to prevent, detect, protect against, and respond to both known and unknown security vulnerabilities—bolstering both privacy and national security imperatives.

Today's Threat Landscape Demands Enhanced Data Security

With the growing volume and sophistication of today's threats, it is critical for organizations to understand the threat landscape and how to properly defend against it. Every member of this committee likely has had a business, bank, school, or local government entity in their state victimized by a cybersecurity attack or data breach. These attacks affect our daily lives—from disruptions of public services like healthcare or emergency services, to leakage of Americans' sensitive data.

Data breaches can result from several factors, including weak credentials, misconfigured security settings, internet-facing software vulnerabilities, and phishing attacks. These incidents can involve significant financial loss and damage to an organization's reputation, and compromise the security of individuals' critical data.

This threat is not subsiding. Instead, adversaries continue to enhance their techniques and increase their sophistication. Bad actors can now execute numerous attacks simultaneously against one company, leveraging multiple vulnerabilities at once. We are also seeing evidence that adversaries are using AI to enhance what we call social engineering attacks—phishing e-mails and voice calls designed to lure users to “click the link” or provide access.

A sobering yet persistent reality of our connected world is that far too many “digital doors” are left open for adversaries to walk through with relative ease.

It is often said the Internet looks very small to an attacker but massive to a defender. After all, an enterprise that closes 99 percent of its digital doors but leaves one open inadvertently may well be destined for a breach. Entities of all sizes, public and private, have historically struggled to understand and manage their digital infrastructure, including phones, laptops, servers, and applications that have been exposed to the internet. In fact, we have found that even sophisticated enterprises actually have twice the number of systems exposed on the Internet than what they were internally monitoring—a visibility gap that gives adversaries the upper hand.

The threat intelligence and incident response division at Palo Alto Networks, known as Unit 42, helps assess and test the security controls of organizations, transform their security strategies with a threat-informed approach, and respond to incidents in record time. In 45 percent of incident response cases led by Unit 42 last year, attackers exfiltrated data in less than a day after compromise, down from 44 days as recently as 2021. Slow response times increase the cost of resolving incidents, and increase the likelihood of sensitive data being compromised.

Complementing our insights from incident response cases, Palo Alto Networks also leverages a capability that indexes the public-facing Internet through the eyes of the adversary to discover exposed systems, vulnerabilities, and misconfigurations. We are increasingly seeing cloud infrastructure as an inviting attack vector for adversaries. In fact, over 80 percent of the exposures we observed were cloud-based, and Unit 42 similarly saw a 115 percent increase in cloud-related incidents in 2023 compared to 2022.

Modern organizations often depend on multiple cloud environments to store, process, and analyze data. The use of diverse cloud services drives many helpful operational efficiencies, but also creates fragmentation—scattering sensitive records across multiple datastores with opaque data flows, and complicated access control mechanisms. Organizations frequently struggle to understand what sensitive data (e.g., customer details, health data, financial information) they actually hold, who can access it, and where it is at risk.

Recognizing these realities, promoting effective data security requires an innovative approach to fortifying cyber defenses, particularly given the constantly evolving threat landscape.

Securing Systems and Data with AI and Automation

Fortunately, AI and automation are proving transformative for network defenders, enabling organizations not only to respond more quickly, but also to more nimbly ingest and analyze security data to proactively harden their networks against attacks.

One of the most promising applications of AI and automation for cyber defense is to significantly uplevel and enhance the capabilities within Security Operation Centers (SOCs). For too long, our community’s most precious cyber resources—people—have been inundated with security alerts that require manual triage, forcing them to play an inefficient game of “whack-a-mole,” while vulnerabilities remain exposed and critical alerts are missed.

Two of the most important metrics for any security operations team are Mean Time to Detect and Mean Time to Respond. As the terms suggest, these metrics provide quantifiable data points for network defenders about how quickly they discover potential security incidents and then how quickly they can contain them to help mitigate their potential impact.

Historically, organizations have struggled to execute against these metrics. A recent *Unit 42 report* that analyzed real-world cloud-related incident response cases found that, on average, security teams take nearly six days to resolve an alert. In contrast, we now see many adversaries moving from compromise to data exfiltration in just hours.

Giving defenders the upper hand requires a new approach that leverages AI-driven SOCs. This technology will be a force multiplier for our cybersecurity professionals and will substantially reduce incident detection and response times.

Early results from deploying this technology on our own company networks have been particularly promising. On average, we ingest 36 billion events daily and use AI-driven data analysis to automatically triage that number down to just eight that require manual analysis. In addition, we have reduced our Mean Time to Detect to just 10 seconds and our Mean Time to Respond to just one minute for high priority alerts.

Early customer benefits have been similarly encouraging. We have already seen a reduction in mean response times from weeks and days to hours and minutes. Such a reduction is critical to stopping threat actors before they can encrypt systems

or steal sensitive information, and for minimizing the impact of an incident. This tool has dramatically improved incident close-out rates from 20 percent pre-deployment to 100 percent post-deployment.

Increased adversarial speed to steal or encrypt data demands rapid detection and response. In order to stay a step ahead of sophisticated adversaries, we must also detect never-before-seen anomalous behavior, not just previously identified attack patterns. AI now gives us the capability to do so—putting network defenders back in the driver’s seat, not a step behind.

Key Data Security Recommendations

As organizations seek to enhance their cybersecurity and data security postures, Palo Alto networks offers the following recommendations:

1. *Ensure complete visibility of attack surfaces:* 75 percent of attacks and breaches fielded by Unit 42’s incident response team result from a common culprit—internet-facing attack surface exposures. Deploying solutions that provide centralized, near real-time visibility can help organizations identify and mitigate vulnerabilities before they can be exploited.
2. *Promote Secure AI by Design:* Enterprises will benefit from capabilities that assist in inventorying AI usage, applying policy controls, and securing apps built with AI.
3. *Leverage the power of AI and automation in network defense* to modernize security operations and reduce the burden on overworked analysts. The latest technology can help organizations drive down key cybersecurity metrics like Mean Time to Detect and Mean Time to Respond, denying attackers the time they need to compromise an organization’s systems or exfiltrate its data. Additionally, technique-based protections mapped to the MITRE ATT&CK Framework can help defenses nimbly evolve in response to adversarial tactics.
4. *Implement enterprise-wide zero trust network architecture:* This is a fundamental security principle that assumes the network is already compromised and implements processes that continuously validate the user, device, application, and data in a controlled manner. Zero trust network architecture creates layers of security that prevent or limit an attacker from successfully moving laterally around the network. This provides victims with more time to detect, properly contain, and remediate the threat.
5. *Protect cloud infrastructure, applications, and data:* With cloud migration accelerating, threat actors will continue to develop tactics, techniques, and procedures designed to target and compromise cloud workloads. Organizations leveraging cloud infrastructure should implement a cloud security program and platform that offers comprehensive cloud-native application protection.
6. *Maintain an incident response plan* to prepare for and respond to cyber incidents, including emerging ransomware tactics like extortion, multi-extortion, and harassment. Organizations that continuously review, update, and test their incident response plans—ideally with input from cybersecurity experts—are much more likely to effectively respond to and contain an active attack. Organizational leadership must elevate cybersecurity as a core part of their overall enterprise risk management strategy.

While there is no silver bullet in cybersecurity, prioritizing these recommendations will materially reduce the risk of falling victim to an attack, more effectively protect data if an attack does occur, and help increase the resilience of the entire cybersecurity ecosystem.

Partnerships and People Remain Critical

It is often said that cybersecurity is a team sport, and partnership is very much in our DNA at Palo Alto Networks—and across the entire cybersecurity industry.

Palo Alto Networks is proud to be a founding Alliance member of CISA’s Joint Cyber Defense Collaborative (JCDC). In forums like these, we share technical threat intelligence on a daily basis through partnerships with U.S. government entities, private sector entities, and other allied nations to support global prevention and response to significant cyber incidents. We are also active members of the NIST National Cybersecurity Center of Excellence projects on 5G, zero trust, and post-quantum cryptography.

It is critical we educate and train the cyber workforce of today and tomorrow with the advanced skills required for meaningful jobs that complement technological innovation. This approach is fundamental to improving our collective cyber defense and enabling data security.

To that end, we have been encouraged to see the impact of several initiatives aimed at broadening access to cybersecurity education, including the Palo Alto Networks Cybersecurity Academy, which offers free and accessible curricula aligned to the NIST National Initiative for Cybersecurity Education (NICE) Framework, to academic institutions from middle school through college. Hands-on experiences with cyber and AI benefit the entire ecosystem as they help to upskill our own workforce as well as that of our customers.

Palo Alto Networks offers several accelerated onboarding programs to diversify the workforce, including the *Unit 42 Academy*, which welcomes new early career participants each August as full-time members of our incident response and cyber risk management teams. We are pleased to report that our 2023–2024 class is 80 percent female.

Taken together, the aspects I've highlighted in my testimony will help address a number of components associated with a holistic approach to data security—technology, processes, and people.

Thank you for the opportunity to testify. I look forward to your questions.

Senator HICKENLOOPER. Thank you, Mr. Kaplan.

Now I'll introduce Prem Trivedi, who is the Policy Director for New America's Open Technology Institute.

**STATEMENT OF PREM TRIVEDI, POLICY DIRECTOR,
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE**

Mr. TRIVEDI. Chair Hickenlooper, Ranking Member Blackburn, members of the Committee, thank you very much for the opportunity to speak with you today.

I'm Prem Trivedi, the Policy Director of the Open Technology Institute at New America, a nonprofit and nonpartisan organization dedicated to realizing the promise of America in an era of rapid technological and social change.

Since 2009, the Open Technology Institute, or OTI, has worked to ensure every community has equitable access to digital technology and its benefits. OTI has long emphasized the need for a strong Federal standard in privacy and data security that protects consumers while retaining sufficient flexibility for innovation.

This takes me to my first point. Data security and consumer privacy are two sides of the same coin. Strong data security safeguards, including minimization, are vital to protecting consumers. And data minimization, as you mentioned in your remarks, is a powerful principle that requires collecting, using, sharing, and retaining only the data necessary to provide a service or a product.

And strong data security safeguards are urgently needed in this era of AI. Training many AI models requires ingesting huge data sets, and as companies race to acquire more data, the pressures to adequately protect it keep increasing. And so a baseline Federal standard on privacy and data security is essential to ethically and effectively regulating AI development.

And I'll add, cybersecurity practitioners also recognize minimization's benefits go beyond consumer privacy, because it can reduce threats posed by breaches and other security incidents.

In short, companies can't misuse data that they don't have. And hackers can't steal data that companies don't have.

My next point is that research shows Americans want strong data security and minimization protections. There's no uniform national standard that protects all types of data, and Americans know that online data collection and tracking of their activities is pervasive.

It's probably why 75 percent of Americans lack confidence that the government will hold a company accountable if it misuses or compromises their data. And all of this concern about data security and privacy is negatively impacting consumer trust in AI and in leading AI companies, many of which are U.S. companies, small and large.

And the good news is that more than two-thirds of Republicans and Democrats support more regulation of companies' data use. And we've been heartened to see the recent reemergence of a credible bipartisan, bicameral legislative proposal on privacy and data security via the American Privacy Rights Act.

The next point I'd like to make is that a strong Federal data minimization regime would replace the broken approach in American privacy governance that relies on notice and consent alone. We know it would take people hundreds of hours to read all the privacy policies that they encounter in just a year. And most Americans, even most privacy professionals, respond to this unfair burden on consumers by clicking "agree" without reading those policies.

This isn't meaningful notice, it's not meaningful consent, and it's not clear either is really achievable in most of our online activities. Data minimization is so important because it shifts the responsibility onto companies, from consumers, to use only what the companies need to provide products or services.

And I want to point out, this is far from a new concept in law or corporate risk management playbooks. So I think we can get the benefits of data minimization without stifling innovation or overburdening smaller companies.

The last main point I'd like to make is that a broad set of best practices in data security should become baseline safeguards across all sectors of our economy. And here's a short list of those best practices.

First, as I've emphasized so far, collect, use, share, and retain only data that's relevant.

Second, whenever possible, use encryption to securely store and process data.

Third, apply strong controls that ensure only the people who should be able to access data can, in fact, access that data.

Fourth, use strong methods for authentication, including multi-factor authentication.

Fifth, further study and standardize over time uses of privacy enhancing technologies.

And sixth, routinely assess and mitigate against data security vulnerabilities, something you've heard from other witnesses as well.

There's no such thing as perfect data security. But these common sense best practices should be requirements in Federal law that are applied flexibly enough to account for different companies' sizes and technical capacity.

In conclusion, data protection is consumer protection, and we need a national legislative framework that requires and incentivizes responsible data stewardship. Continued U.S. leadership on AI requires Congress to address the consumer trust gap. And we

appreciate the Committee’s bipartisan leadership on data security and privacy.

Thank you again for the opportunity to testify before the Subcommittee. I look forward to your questions.

[The prepared statement of Mr. Trivedi follows:]

PREPARED STATEMENT OF PREM M. TRIVEDI, POLICY DIRECTOR, NEW AMERICA’S
OPEN TECHNOLOGY INSTITUTE

Introduction

Chair Cantwell, Ranking Member Cruz, Subcommittee Chair Hickenlooper, Ranking Member Blackburn, and Members of the Committee, thank you for the opportunity to offer testimony today on how strong data security safeguards protect consumers. A Federal standard for data security, and particularly for data minimization, is critical to protecting American consumers and American companies from the over-collection of data, subsequent misuse of such data, and the harms of data breaches.

My name is Prem Trivedi, and I am the policy director of the Open Technology Institute at New America, a nonprofit and nonpartisan organization dedicated to realizing the promise of America in an era of rapid technological and social change.¹ Since 2009, the Open Technology Institute (OTI) has worked at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.²

OTI has long emphasized the need for strong, common Federal standards in privacy and data security that protect consumers while retaining sufficient flexibility for innovation. We have been heartened to see the reemergence of a credible bipartisan legislative proposal on privacy and data security via the American Privacy Rights Act (APRA).³ Data security and consumer privacy are two sides of the same coin. Perhaps no principle better illustrates that fundamental truth than data minimization, which requires companies to collect, use, share, and retain only what they need to provide a product or service. Strengthening Federal protections for privacy and data security is vital to protecting Americans, a key foundation of responsibly regulating artificial intelligence, and an important part of safeguarding our economic and national security. We at OTI commend the Subcommittee for its leadership in spotlighting how data security and data minimization play an essential role in protecting consumers and data.

My testimony makes four key points:

1. Strong data security safeguards, including data minimization, are essential to protecting consumers.
2. Consumer research shows that Americans want stronger data security and privacy laws, including the protections of data minimization.
3. Data minimization requirements in a Federal privacy law could fix the broken notice and consent approach to U.S. privacy law.
4. Codifying a broader set of data security practices in Federal law would also meaningfully protect consumers’ and companies’ data.

I. Strong Data Security Safeguards, including Data Minimization, Are Vital to Protecting Consumers

“Data minimization” may seem like a dry and technocratic-sounding term. But, at its core, it is a powerful principle for collecting, using, sharing, and retaining only the data that is necessary to provide a service or product. Data minimization is an essential element of effective privacy and data governance that protects people and organizations from misuse and mitigates the harms of data breaches. And it is already a well understood, common requirement in international, federal, and state laws and regulations. In addition, data minimization is a core part of internal company rules and risk assessments, but it is not consistently applied with sufficient rigor. A brief examination of first-and third-party tracking on the Internet powerfully illustrates why we need a common national baseline for data minimization.

¹ *Our Story*, New America, <https://www.newamerica.org/our-story/>

² *About*, New America’s Open Technology Institute, <https://www.newamerica.org/oti/about/>

³ *American Privacy Rights Act of 2024 (discussion draft)*, https://d1dh6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf.

The average modern web page or smartphone application collects information about you—like the browser you use, your IP address, metrics about how you engage with the site or app, and any information you actively provide. This is “first-party” data collection. But a web page also uses code from other companies or entities, which are referred to as third parties—sometimes dozens of them. This type of code may be placed on a website to improve your experience or to provide a service like web analytics for the site’s owner. Each of those third parties is in a position to track that site’s visitors and collect and retain a broad range of data about them. If a third party’s code is included on multiple websites, then you can be tracked as having visited both pages, and data brokers can potentially bundle and sell that data to entities ranging from domestic and foreign governments to insurance companies and credit bureaus.

Even if a third party is providing a legitimate service, it is almost impossible for the average person to know if that is the case because all of this code is loaded silently in the background. Finding out which third parties a site loads requires special tools and then a further step of researching the services those third parties provide. While it might be feasible to investigate a site like *senate.gov*, which only loads code from two third parties, it is simply not practical to do that on very popular pages, like mainstream news websites—many of which load code from dozens of third parties. Similarly, developers of smartphone apps may include third-party libraries that can analogously track users via their devices and sometimes their activity in other apps, which is known as “cross-app tracking.”

There are certainly companies in this ecosystem that follow responsible privacy practices, but many others do not show the same regard for privacy and data security. Strong data minimization rules would restrict both first-party and third-party data collection and use. They would alleviate some of the unrealistic responsibility forced onto website visitors and app users to figure out how their data is collected and used and which third parties may be tracking them. Strong rules would also bolster public trust if people knew that a Federal law reasonably minimized the amount of data about them that could be gathered, used, and stored. *Companies cannot use data that they don’t have.*

Cybersecurity practitioners recognize the importance of minimization. Consistent reductions in data collection and use would significantly reduce the threats posed by breaches and other security incidents. Responsible data minimization also lowers the possible harms when companies get hacked. A common data security maxim is “If you can’t protect it, don’t collect it.”⁴ A common privacy maxim is “Collect and use only what you need.” And here is a synthesis that I will borrow from another civil society organization: “You don’t have to protect what you don’t collect.”⁵ This perfectly illustrates how data minimization is a cornerstone of protecting consumers and companies, safeguarding privacy, and securing data. *Hackers cannot steal data that companies do not have.*

The central role of data minimization in data security is even clearer when we think about how some of Americans’ most sensitive data is held by institutions like schools and hospitals. These organizations may have varying levels of technical capacity to implement data security measures. Although Federal privacy laws cover sectors like health, finance, and education, the reality is that virtually every institution is likely to hold and use sensitive data—including data not covered by data security or privacy laws. A strictly sectoral approach to data security and privacy leaves unprotected many institutions and Americans who need a baseline level of support from a strong Federal standard for data minimization and other security practices.

In addition, the need for robust data minimization and other security provisions is increasingly evident in this era of artificial intelligence (AI). The training of many AI models—particularly powerful “foundation” models designed to be adapted for a variety of purposes—requires the ingestion of huge data sets. As companies race to acquire more and more data, the pressures on privacy and data security are becoming even more acute.⁶ Although there appears to be broad consensus on the need to regulate AI, public debate sometimes overlooks the fact that a baseline Federal

⁴ Richard Bejtlich, *New cybersecurity mantra: “If you can’t protect it, don’t collect it.”*, Brookings, Sep. 3, 2015, <https://www.brookings.edu/articles/new-cybersecurity-mantra-if-you-cant-protect-it-dont-collect-it/>.

⁵ John Davissan, *Data Minimization: A Pillar of Data Security, But More Than That Too*, Electronic Privacy Information Center, Jun. 22, 2023, <https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/>.

⁶ Cade Metz, Cecilia Kang, Sheera Frenkel, Stuart A. Thompson, and Nico Grant, *How Tech Giants Cut Corners to Harvest Data for A.I.*, New York Times, Apr. 8, 2024, <https://www.nytimes.com/2024/04/06/technology/tech-giants-harvest-data-artificial-intelligence.html>.

standard on privacy and data security is foundational to ethically and effectively regulating AI development.

II. Research Shows Americans Want Strong Data Security and Minimization Protections

We don't need to take data protection professionals' word about the importance of protecting data security and privacy. Consumer research by companies and non-profits shows that Americans feel a lack of control over their data and are unsure of what data companies collect from them and how they use it. This environment of uncertainty and mistrust leaves them wanting stronger privacy and data security protections.

According to a 2023 report from the International Association of Privacy Professionals, nearly 68 percent of consumers globally said they were somewhat or very concerned about their privacy online. And only 29 percent of consumers surveyed said it was easy for them to understand how a company protects their personal data.⁷ A 2023 KPMG survey of 2,000 Americans found that 86 percent of those surveyed said their data privacy is a source of growing concern.⁸

Consumers are similarly worried about data security. A 2024 Deloitte study reveals that about 60 percent of survey respondents worry that their devices are vulnerable to security breaches and are concerned that organizations or people could track them through their devices.⁹ These are not abstract fears. A third of the survey respondents said "they experienced at least one type of breach or scam in the past year, and 16 percent fell victim to two or more kinds."¹⁰

In the United States, as the Committee knows well, we have sector-specific data security and privacy laws at the Federal level but no uniform national standard that applies to all Americans and establishes a baseline for protecting all types of data.

Perhaps that helps to explain why, according to a 2019 Pew Research study, 72 percent of "Americans report feeling that all, almost all or most of what they do online or while using their cellphone is being tracked by advertisers, technology firms or other companies."¹¹ It surely is part of the reason why 75 percent of Americans are not confident that the government will hold a company accountable if it misuses or compromises their data.¹² According to Pew's updated research in 2023, the concerns have only grown worse. Last year, 67 percent of Americans reported that "they understand little to nothing about what companies are doing with their personal data."¹³

All of this concern about data security and privacy is negatively impacting consumer trust in AI technology and leading AI companies. According to a Cisco survey, 62 percent of global consumers are concerned about the business use of AI today, and 60 percent say that the use of AI by organizations so far has already eroded their trust.¹⁴ American consumers are no exception to the global trend. When surveyed last year, 70 percent of Americans who have heard about AI have little to no trust in companies to make responsible decisions about how they use it in their products.¹⁵

Another statistic demonstrates the loss of agency that Americans feel over their data and illustrates why data minimization and other data security measures are

⁷Müge Fazlioglu, *Privacy and Consumer Trust*, IAPP, Mar. 2023, <https://iapp.org/media/pdf/resource-center/privacy-and-consumer-trust-report-summary.pdf>.

⁸Corporate data responsibility: Bridging the consumer trust gap, KPMG, 2023, <https://kpmg.com/us/en/articles/2023/bridging-the-trust-chasm.html>.

⁹Jana Arbanas et al., *Data privacy and security worries are on the rise, while trust is down* [2023 Connected consumer survey, Deloitte, 2023, <https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html#explore>.

¹⁰*Id.*

¹¹Brooke Auxier, Lee Rainie et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* at p. 6, Pew Research, Nov. 15 2019, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf.

¹²Brooke Auxier, Lee Rainie et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* at p. 9, Pew Research, Nov. 15 2019, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf.

¹³Colleen McClain, Michelle Faverio et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research, Oct. 18, 2023, <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.

¹⁴Generation Privacy: Young Consumers Leading the Way Cisco 2023 Consumer Privacy Survey, Cisco, Oct. 18, 2023, <https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html>.

¹⁵Colleen McClain, Michelle Faverio et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research, Oct. 18, 2023, <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.

so important in restoring Americans' trust in their government's ability to require responsible data stewardship. Although 78 percent of Americans trust themselves to make "the right decisions about their personal information," a majority doubt that anything they do will make much of a difference. Only about one in five Americans are confident that those who have their personal information will treat it responsibly.¹⁶

These studies are just a small sampling of consumer research that reveals deep-seated concerns—both globally and in the United States—about privacy, data use, and trust in AI companies. But Americans are also clear about the solutions to this problem, with 72 percent of Americans wanting more regulation of companies' data practices.¹⁷ Notably, this support is bipartisan, with 68 percent of Republicans and 78 percent of Democrats expressing this view.¹⁸ And most Americans are also clear that the specific path forward involves data minimization and other data security protections. Research consistently shows that Americans are concerned about how much data companies collect from them.

Interestingly, some studies suggest that company leaders understand the trust deficit among their consumers and broadly agree on the path forward. A 2023 KPMG survey of 250 business leaders found that 70 percent said their company increased data collection over the previous year.¹⁹ One out of three business leaders surveyed said that consumers should be concerned about how *their* company uses personal data. Tracking consumer sentiment, 62 percent of leaders said their company should do more to protect their consumers' personal data.²⁰

III. Strong Federal Data Minimization Rules Could Fix the Broken Notice and Consent Privacy Paradigm in the United States

A strong Federal data minimization regime would respond to consumer concerns and finally replace the broken notice and consent approach that has defined American data security and privacy governance for decades. The "notice and consent" approach requires private entities to notify individuals and ask for their permission before collecting and utilizing their personal data.²¹ These notices often take the form of privacy policies. But it would take people *hundreds* of hours to read all the privacy policies for websites and applications that most of us encounter in just a year.²² In 2019, one in five Americans said they often or always read privacy policies,²³ and even that figure seems surprisingly high. In 2023, a majority of Americans responded to this unfair burden on consumers by just clicking "agree" without reading privacy policies.²⁴ This isn't meaningful notice, it isn't meaningful consent, and it is not clear that either is achievable in the course of most of our online activities.²⁵ Enter data minimization, which shifts the responsibility onto companies to

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ Corporate data responsibility: Bridging the consumer trust gap, KPMG, 2023, <https://kpmg.com/us/en/articles/2023/bridging-the-trust-chasm.html>.

²⁰ *Id.*

²¹ Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, New America's Open Technology Institute, Mar. 23, 2020, <https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/> ("Notice and consent is too weak in practice to meaningfully shield individual privacy. Instead, we need comprehensive privacy legislation that will empower individuals with explicit user rights over their data, and provide strict limits on how private entities handle that data.").

²² Geoffrey A. Fowler, *I Tried to Read All My App Policies. It Was 1 Million Words*, Washington Post, May 31, 2022, <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>; Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543–568, <https://kb.osu.edu/server/api/core/bitstreams/a9510be5-b51e-526d-aea3-8e9636bc00cd/content>.

²³ Brooke Auxier, Lee Rainie et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research, Nov. 15 2019, <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>.

²⁴ Michelle Faverio, *Key findings about Americans and data privacy*, Pew Research, Oct. 18, 2023, <https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/>.

²⁵ Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013) https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications; David Medine and Gayatri Murthy, *Companies, not people, should bear the burden of protecting data*, David Medine and Gayatri Murthy, Brookings, Dec. 18, 2019, <https://www.brookings.edu/articles/companies-not-people-should-bear-the-burden-of-protecting-data/>.

exercise restraint by collecting and using data only that they need to provide their products or services.

Right now, the U.S. legislative regime for data security is fragmented in ways that make consumers more vulnerable and require companies to develop complicated compliance programs in the absence of clear national rules of the road. In broad terms, a credible Federal data minimization standard would require that companies only collect and process data that is reasonably necessary for the products and services that they offer, in addition to fulfilling other permissible purposes like data security and protection against fraud. A Federal data privacy and security law would make clear that the obligation to minimize data applies to all aspects of the data life cycle: data collection, use, transfer, and retention. Congress has made progress in this respect, most recently in the discussion draft of the American Privacy Rights Act (APRA), which would establish a data minimization regime and robust data security requirements.

We at the Open Technology Institute believe in the power of digital technology to produce transformative innovation that serves the public interest. However, the costs of continuing to operate without a reasonable Federal standard on data minimization—to American consumers, American companies, and the health of our economy—are simply too high. The proposed solution—a comprehensive Federal privacy law rooted in data minimization and data security obligations—would not overburden industry.

Data minimization is not a rigid concept that by itself would stifle innovation or hamstring companies, whether large or small, incumbent or start-up. Properly applied, data minimization can reduce security concerns, protect user data, and lead to better products and services.

Data minimization is not a new concept that is difficult to incorporate in Federal law. Minimization and other well-established data protection principles stem from an earlier era of U.S. leadership on responsible data governance. The U.S. Department of Health, Education, and Welfare, in 1973, published a landmark report that established a set of five Fair Information Practices (FIPs).²⁶ Those five principles have been further developed into principles like the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, which include the core requirements of data minimization. Those requirements, in turn, have been incorporated into legislation around the world, including Europe’s General Data Protection Regulation (GDPR), Brazil’s General Personal Data Protection Law (LGPD), and India’s Digital Personal Data Protection Act (DPDPA).²⁷ Each of these laws takes a slightly different approach to minimization, but they all adopt the principle as a legal requirement. Against this global backdrop, a comprehensive U.S. Federal law on data protection and privacy is conspicuously absent.

Data minimization is also widely understood by companies as a principle of risk management, but the application across companies and sectors is inconsistent. Federal codification of data minimization rules would not be seen as a novel regulatory requirement. Major U.S. tech companies, for example, already include data minimization in their privacy and data governance frameworks.²⁸

IV. Strong Federal Data Security Standards Are Essential to Addressing Variations across Sectors and Data Types

OTI focuses considerably on data minimization because it is often an underappreciated aspect of securing data and protecting consumers, but there are also other basic best practices in data security that should be required as a baseline across all sectors of the economy. Strong Federal legislative requirements could require companies and other organizations to do the following:

²⁶U.S. Dep’t. of Health, Education and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens (1973), <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>.

²⁷Using the OECD Privacy Guidelines as an illustration, the following principles collectively fall under the broader umbrella of data minimization: collection limitation, purpose specification, and use limitation. See *OECD Privacy Guidelines* (last amended Oct. 2013), Organisation for Economic Cooperation and Development, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.

²⁸See, e.g., Meta, *Privacy Progress Update (Privacy Review)*, <https://about.meta.com/privacy-progress/#how-we-do-it> (listing data minimization as a core privacy principle); Google, *Your privacy is protected by responsible data practices*, <https://safety.google/privacy/data/> (noting that data minimization “limit[s] the personal information that is used and saved”); Google, *Our Privacy Principles*, <https://safety.google/principles/> (listing as the fourth principle “We reduce the data we use to further protect your privacy.”).

- *Securely store and process data.* When feasible, given the intended uses of the data, it is a best practice to encrypt data at rest (stored data) and data in transit (data being transmitted between devices and servers).
- *Apply strong access controls, which can be implemented through technical controls and administrative rules.* It is critical to ensure that only the people who need to be able to access data actually can access it.
- *Use strong methods for authentication and identity management.* Companies must ensure that data access is accompanied by robust authentication requirements, which include but are not limited to using appropriately strong passwords in combination with multi-factor authentication. Unfortunately, many data breaches take place because weak or default passwords enable the success of password-guessing efforts.²⁹
- *Retain only data that is still needed by periodically reviewing data sets for relevance and deleting what is no longer needed.* As discussed in Sections I–III, minimizing the amount of available data is an important safeguard against misuse and mitigates the harms from data breaches.
- *Standardize privacy-enhancing technologies.* Advancements in encryption and increasingly secure computing environments have led to a new generation of data processing tools. Technologies like multi-party computation and zero-knowledge proofs allow for data to be processed in a way that all the data remains encrypted and no private information is disclosed. These and other privacy-enhancing technologies should become the standard for processing data.
- *Routinely assess and mitigate against data security vulnerabilities at the device, network, and application levels.* Companies should not only regularly apply updates and security patches for their hardware and software, but they should also be aware of and implement other common security practices, like network segmentation.³⁰

There is, of course, no such thing as perfect security in either the digital or physical worlds. But common-sense best practices like these should be standard requirements in Federal law, so long as they are applied with enough flexibility to account for variation in organizations' size and capacity to develop sophisticated data security programs.

Conclusion

Americans want strong and consistent protections for their data. They realize that their data can represent the most sensitive aspects of their lives. Data protection is consumer protection, and this committee is deeply aware of the need for companies to serve as responsible stewards of data—personal or otherwise.

Rapid advances in artificial intelligence serve as a reminder that now is the time to ensure a strong, common national standard for data security and privacy. We appreciate the Committee's bipartisan leadership on privacy and data security legislation. OTI looks forward to working with Members of Congress to help advance strong privacy and data security protections into law.

Senator HICKENLOOPER. Thank you very much.

I'll now go to Mr. Parker. I forget—you're the director of—Senior Director of Security Industry Association. Thank you for being here.

STATEMENT OF JAKE PARKER, SENIOR DIRECTOR OF GOVERNMENT RELATIONS, SECURITY INDUSTRY ASSOCIATION

Mr. PARKER. Good afternoon, Chairman Hickenlooper, Ranking Member Blackburn. Thank you for the opportunity to participate in today's hearing.

²⁹Verizon Business, *2024 Data Breach Investigations Report* p. 43–44, <https://www.verizon.com/business/resources/T990/reports/2024-dbir-data-breach-investigations-report.pdf>; *State of Security 2024: The Race to Harness AI*, Splunk, https://www.splunk.com/en_us/form/state-of-security.html (“... attackers often use older vulnerabilities, default passwords, and other low hanging fruit to target organizations, so a commitment to cyber hygiene is more important than ever.”).

³⁰See, e.g., *What is Network Segmentation?*, Cisco, <https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html#how-segmentation-works>.

Again, I'm Jake Parker with the Security Industry Association. This is a nonprofit trade association representing more than 1,500 companies that provide products for protecting lives, property, businesses, schools, and critical infrastructure throughout the Nation.

So data security is essential to the operation of security systems and services, and our members are committed to protecting personal data, whether it is consumer or operational data. Practices like data minimization and privacy-by-design, enhance the end-to-end security needed for successful implementation of many types of these products.

For example, when it comes to access control and video systems, features like data encryption, which we talked a bit about here, permissions-based access, decentralized data storage, edge device processing, audit capabilities, and data deletion schedules all serve to limit the availability of data for potential misuse, and limit the usefulness of data if it is compromised.

In another example, our members provide the multi-factor authentication and remote identity proofing services that are becoming essential to preventing identity theft and fraud as attackers become more sophisticated.

These advanced technologies provided by our industry, especially biometrics, are providing higher-assurance authentication, while reducing exposure of passwords and other personal information that is far more vulnerable to exploitation by identity thieves and cyber hackers.

As we've heard from the other witnesses, there are very serious and rapidly increasing threats to data security that must be addressed. And beyond technical standards, product features, best practices, and security tools, the right—having the right public policies in place will also address data privacy and security. There's a key role for those.

So states like Colorado, Texas, Tennessee, and by my count, by the end of this month, there will be a total of 19 states that have enacted comprehensive data privacy and security laws, which cover over 160 million Americans, or almost half the population.

However, having a uniform national standard could provide more benefits to businesses and consumers, while further enhancing data security. And a national standard is something our members support. We've been following the renewed discussions here in Congress regarding the development of such a standard, and we are encouraged by the progress.

In this, it's essential that data can continue to be utilized as needed for safety and security purposes. For example, our members and their customers are often the first to raise the alarm in emergencies, where having the right data helps law enforcement and other responders get to where they need to be as quickly as possible.

And also mentioned earlier, there are many technologies used for authentication that will be essential to accomplishing the goals of the draft proposal that we are looking at in section 9, which I think was mentioned earlier.

So having a uniform and workable national standard requires strong state and local preemption to avoid layering additional requirements. This is really important to our industry.

It also needs to limit risks to businesses from opportunistic abusive lawsuits, which we've certainly seen in some jurisdictions over privacy matters. And need to make sure that we accomplish those two objectives in what we put forward.

So I appreciate you holding this hearing, and your leadership, and putting a spotlight on data security. And as an organization, we're doing what we can, through our data privacy advisory board and our cybersecurity advisory board in particular, to provide key resources and urge adoption and best practices for data security in our industry, as I outlined in my written statement.

Again, thank you for the opportunity to participate. And on behalf of SIA and our members, we look forward to continue working with you on these issues.

[The prepared statement of Mr. Parker follows:]

PREPARED STATEMENT OF JAKE PARKER, SENIOR DIRECTOR OF GOVERNMENT
RELATIONS, SECURITY INDUSTRY ASSOCIATION

Chairman Hickenlooper, Ranking Member Blackburn and distinguished members of the Committee, my name is Jake Parker, Senior Director of Government Relations for the Security Industry Association (SIA). SIA is a nonprofit trade association representing more than 1,500 companies that provide safety and security products essential to protecting lives, property, businesses, schools, and critical infrastructure throughout the U.S. and employ thousands of technology leaders.

Best Practices and Commitment of the Security Industry to Data Protection

Data security is essential to the delivery and operation of security systems and services. SIA members are committed to protecting personal data, whether it is consumer or operational data. Through our Data Privacy Advisory Board¹ and Cybersecurity Advisory Board,² SIA is encouraging members to implement best practices for data security by providing resources like our *Privacy Code of Conduct*,³ *Ten Tips for Implementing Data Privacy*,⁴ *How to Counter AI-Driven Cybersecurity Threats to Physical Security Products*,⁵ and enterprise security risk management (ESRM) strategies for our industry.⁶

It is critical to provide our customers with tools and strategies that address risks both inside and outside their organizations. Data minimization—in the operational sense—is important to the secure implementation of key security products like access control and video security systems. Across many applications, privacy-by-design also enhances end-to-end security. Features like strict permissions-based data access, de-centralized data storage, encryption of data in transit/at rest, customer-only access to cloud-hosted data, “edge” device processing, user audit capabilities and data retention schedules all serve to enhance privacy and security by limiting the availability of data for potential misuse and limiting the usefulness of data if it is compromised. Our members provide technology for multi-factor authentication and high assurance identity authentication, including remote identity proofing services that are essential to meeting today's (and tomorrow's) identity theft and fraud prevention needs. And in emergency communications applications, our members are the first to raise the alarm in an emergency, using the right data to help law enforcement and other first responders get to where they need to be as quickly as possible.

Key Role of Authentication Technologies in Data Security

Technology innovations are playing a key role in enhancing data security. Biometric technologies are a good example as they are becoming increasingly important for many types of secure transactions. When provided as an option to consumers to authenticate identity for example, these technologies provide more convenience and

¹ <https://www.securityindustry.org/committee/data-privacy-advisory-board/>

² <https://www.securityindustry.org/committee/cybersecurity-advisory-board/>

³ <https://www.securityindustry.org/report/sia-privacy-code-of-conduct/>

⁴ <https://www.securityindustry.org/report/ten-tips-for-implementing-data-privacy/>

⁵ <https://www.securityindustry.org/2023/10/05/how-to-counter-ai-driven-cybersecurity-threats-to-physical-security-products/>

⁶ See *Security Convergence 2024*, <https://www.securityindustry.org/wp-content/uploads/2024/02/SIA-Security-Convergence-2024.pdf>

additional data security at the same time. Biometric technologies offer faster and higher-assurance authentication while reducing the transfer or exposure of personal information that is more vulnerable to exploitation. In fact, there is natural cryptography for biometric data that prevents identity hacking even if that data is stolen, and naturally serves to limit unauthorized use by third parties. It is far less vulnerable than information like social security numbers and passwords, that is easily exploited by identity thieves and cyber-attackers.

Biometric software creates a numerical “template” based on an individual’s physical characteristics to compare with a template or templates already enrolled in a database or on a device. This numerical string of data (based on “mathematical vectors”) is created and readable only within that specific software. Contrary to a common misunderstanding that such data is unchangeable and more vulnerable, this data is in fact infinitely “changeable,” both software version to software version and in that templates will be slightly different each time they are created by the software (due to varying positions of a finger placed on a sensor or varying photography conditions for example). Templates are then “matched” based on mathematical similarity with the enrolled information.

A biometric template itself does not contain any personally identifiable information, and it is unusable outside of the software system that created it. Importantly, a template cannot be used to re-create the image (of a fingerprint, face, etc.) or physiological feature that it was derived from. Since each provider uses a different process to create and compare templates unique to that proprietary system, a template created in one system cannot be used in another. While such data would be useless if sold or shared, its collection, storage and processing should optimize privacy and security using encryption and other best practices in securing sensitive information.

Importance of Uniform Data Privacy Rules in Enhancing Data Security

We are following with interest recent renewed discussions in Congress regarding the development of a Federal data privacy standard that would bolster data security through data minimization among other elements. Such a standard could potentially provide tremendous benefits if it applies clear, workable and uniform rules that are predictable for both businesses and consumers. We believe any national standard must ensure the continued functionality and effectiveness of safety and security technology applications and the benefits to society. This means ensuring data can be collected and processed as needed for these purposes, as well as ensuring requirements do not inadvertently create new security risks.

Uniformity is essential. Express preemption of all state and local laws related to data privacy and security that is iron-clad against challenge in court is necessary to avoid the potential for adding layer upon layer of complex requirements. Recent legislation in Colorado is just one example of layering that could continue to occur without strong preemption. Despite the Colorado Privacy Act having just become effective in July 2023, the legislature recently passed a measure⁷ imposing an extra layer of different requirements specifically for biometric data despite existing regulation of this data under the CPA. The measure dramatically expands applicability both to small businesses and to employee data, which had previously been out of scope under the CPA. The potential increasing complexity of such state-by-state rules covering an ever-expanding set of data and number of entities that must comply is likely to cause confusion and slow business decisions both locally and nationally. The same goes for potential non-preemption of state and local laws providing a private right of action to enforce data privacy and security requirements.

A national data privacy law should limit the potential for abusive lawsuits by plaintiffs’ attorneys seeking “sue-and-settle” outcomes, as the applicability to nearly all sectors of the economy could provide an irresistible target. We have seen the impact firsthand under the deeply flawed Illinois Biometric Information Protection Act (BIPA) where such lawsuits have been filed against many of our members and their customers in Illinois, even though no actual consumer harm is alleged. 88 percent of the cases have been related to biometric timekeeping processes for hourly employees to clock in to work, but many others have involved security and identity verification services.⁸ As a result, today there are many industry products that suppliers refuse to provide to Illinois businesses and consumers due to the litigation risk, despite wide availability elsewhere, cutting off access to effective technologies

⁷ <https://leg.colorado.gov/bills/hb24-1130>

⁸ <https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf>

for home and building security, workplace safety, security investigations and emergency response.

Any national standard should also limit the potential for layers of conflicting requirements and/or frivolous litigation stemming from local jurisdictions enacting their own data privacy laws. For example, the latest class action lawsuit under the City of New York's 2021 Biometric Identifier Information Law,⁹ a major retailer is being sued over allegations it is "profiting from" data in violation of the measure, simply due to use of security systems to protect employees and customers, and limit victimization by organized retail crime gangs.¹⁰ And, during the City of Baltimore's 18-month ban on use of certain biometric technologies by businesses that ended in 2022, a popular rideshare service was forced to discontinue its remote authentication of drivers in the area, with potential impact to rider safety. Again, such issues can be addressed by full and uniform state and local preemption.

Conclusion

On behalf of SIA, I appreciate the opportunity to provide collective input from our industry on the important matter of data security. We are committed to working in partnership with Members of Congress in addressing related areas of public policy. I will do my best to answer any questions you may have. However, if there is any information requested that I cannot provide today, I will be happy to work with our members to provide helpful information.

Senator HICKENLOOPER. Great.

Thank you all again for being here. I realize how busy you all are, and it's some sacrifice. You come and share your information, your wisdom, your data with us.

Let me start off with you, Mr. Trivedi. Lincoln famously said, "With public sentiment, nothing can fail. Without it, nothing could succeed." Various states have established their own laws, soon to be 19 states that will pass their laws. And this is all about how—what types of data businesses can collect, how consumers should be notified.

Consumers can be better protected. I think businesses can more fairly compete when there are clear, consistent rules of the road, and especially for small businesses, I think this is especially important.

So Mr. Trivedi, how do you believe a national standard for data minimization and securing data ultimately benefits customers and their privacy? And maybe a thought about how we get the word out to them to get that public sentiment behind us.

Mr. TRIVEDI. Thanks so much for that question, Chair Hickenlooper.

I mean, I'd start by saying Americans know that their data represents the most sensitive aspect of their lives, and that's why they're clamoring for strong protections for it. And as you've said, a national standard would set equal protections for all Americans, but also set uniform expectations for all companies, which is something that they have been clamoring for as well.

And that kind of clarity in the regulatory environment is sorely needed, because the U.S. legislative regime for data privacy and security is fragmented in ways that make consumers more vulnerable and then require companies—and this is particularly burdensome, I think, for, for smaller companies—to develop complicated compliance programs in response to state patchworks and in the absence of clear national rules of the road.

⁹ <https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCAAdmin/0-0-0-42626>

¹⁰ <https://findbiometrics.com/t-mobile-profited-from-biometric-security-by-preventing-theft-law-suit-alleges/>

I think I would also add to your question about small business in particular, that many of these small businesses do not want to be hoovering up as much data as possible to run their business. But because there aren't sort of credible, strong, inflexible national standards, they may feel as though there's a competitive disadvantage if they're not collecting as much data as possible.

That, as we've heard, puts consumers at risk. It also puts those companies at risk.

And so I think that a data minimization approach and a data security approach that's common at the Federal level helps these companies do what they want to do, which is be responsible data stewards.

Senator HICKENLOOPER. Well, I agree, but certainly hope you're right. Certainly AI has created a fascination with the value of all data, and there seems to be a little bit of a race on. Minimization is not quite appearing as frequently as it had been since AI has gotten more currency.

Mr. Kaplan, on a bipartisan basis, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act a couple years ago to require critical infrastructure operators to quickly report cyber incidents, so we can understand the threat landscape as it changes.

The FTC has also investigated and issued penalties against companies it found were unfair or deceptive in their data security practices after the consumer data was exposed.

Gathering and sharing information about specific ongoing attacks, as well as the broader industry trends, helps us establish the defenses to prevent future incidents, especially, obviously, data breaches across sectors.

So in your experience, Mr. Kaplan, which vulnerabilities do you think are most important to address in order to prevent data—prevent criminals from assessing—or accessing consumer data?

Mr. KAPLAN. Thank you, Senator. That's a very great question. So in our experience—and conveniently, every year, Palo Alto Networks publishes an incident response report, which provides an aggregated summary of the key trends that we've seen and how adversaries are looking to break into systems across the country.

In this past year, we found that Internet-facing software vulnerabilities actually surpassed phishing attempts as the primary vector for attacks to take place. These are essentially open doors that are available on public websites that haven't been patched through updates or upgrades to software and systems. As a result, the adversaries are able to leverage these vulnerabilities with relevant ease to gain entree into these systems.

To that vein, all vulnerability should be taken seriously. But the one vulnerability that we've noticed that is particularly troublesome is called a remote desktop protocol, or an RDP vulnerability. This in particular, if exploited, these can provide threat actors and attackers easy access to a deep level of administrative privilege into a victim's system to better and quicker exfiltrate data. These RDP vulnerabilities will unlock the keys to the kingdom, if you will. So they're a particular concern for our company.

With adversaries growing increasingly sophisticated, it's critical that we make it as difficult as possible through layered defenses,

and some of the best practices that I identified in my opening statement with regard to zero trust architecture, to prevent attackers from moving laterally across the system, and to close those open doors, and to have better understanding and visibility into your relative attack surface.

Senator HICKENLOOPER. And we'll get back to some of that. The—you know, the danger of any hearing like this is we do call attention to some of those open doors, but increases your commercial activity in all of yours.

I'm going to turn it over to my Vice Chair, Senator Blackburn, for some questions.

Senator BLACKBURN. And thank you all so much for your testimony. And I appreciate getting your perspectives on this.

I want to start with GDPR. I mentioned that in my opening remarks. And let me ask you, are each of you involved in some way in the EU? Are your companies involved in some way in the EU? A show of hands is fine. OK, so two of you are. Mr. Trivedi, you're trying to decide if you are or not?

Mr. TRIVEDI. Only to say that we're not a company, so no business in the EU, but we're a nonprofit that's certainly tracking.

Senator BLACKBURN. Right. Yes. Mr. Lee, likewise.

What—as we look at this, and as I mentioned, our friends in the EU know they went a little bit too far. But companies already have these protocols in place to meet the GDPR standard. So as you look at what they have done in the EU, and Canada has a law, and New Zealand has a law, and Australia has a law, all protecting their citizens in the virtual space.

Mr. Lee, start with you, and just go down the line, what should be the lessons that we learned and what should we take away from the GDPR experience? Go ahead and just very quickly so I can work on through my questions.

Mr. LEE. The things that I think they got right do deal with some of the more technical aspects of making sure that you are having the programs that you need in place, and that they meet the risk that you are facing. So it's not a prescriptive necessary—necessarily standard, but it's you have to assess and report. And then when there is a data breach, you have to report that to the data authority for that country.

Senator BLACKBURN. So their assessment reporting mechanism—

Mr. LEE. Yes.

Senator BLACKBURN.—you would say they got it right?

Mr. Kaplan.

Mr. KAPLAN. Thank you, Senator. That's a great question. I would say from a macro level, the things that they got right are sort of a uniform standard.

Senator BLACKBURN. Right.

Mr. KAPLAN. Regulatory complexity across multiple markets just increases costs. And from a cybersecurity perspective, the sources that—and the resources that are dedicated to responding to incidents should be operationally responding to incidents rather than looking at regulatory responses.

Senator BLACKBURN. As I say, we need one set of rules for the entire Internet ecosystem, with one regulator. Yes.

Mr. KAPLAN. Predictability and lessening regulatory complexity—

Senator BLACKBURN. Yes.

Mr. KAPLAN.—is one of the hallmarks.

Senator BLACKBURN. It's a good thing, isn't it?

Mr. Trivedi.

Mr. TRIVEDI. Thank you, Senator, for the question. I think the first lesson is something you highlighted, which is moving swiftly to establish that uniform standard. That's something we should—

Senator BLACKBURN. Yes.

Mr. TRIVEDI.—should emulate. I think it's worth saying GDPR has probably not been strong enough on data minimization, that I think the regime we're hopefully working toward here in the United States could do it better. I think GDPR arguably gives too much deference to companies to decide what minimization means. And I think while we should have sort of a reasonableness thing and a flexibility, we need a strong and flexible approach, I think there's an opportunity for an American approach that's different and that works for us.

Senator BLACKBURN. OK.

Mr. Parker.

Mr. PARKER. I would say the—I mean, the emphasis on reasonableness, proportionality, and consent is very similar to what a lot of the states have done already. I see the similarities between those two, which obviously was pointed out, is a little bit different than what the proposal we're talking about now at the Federal level is.

But just based on what I've also—some feedback from members we've had is, there has definitely been an issue with conflicting interpretations over time from the national data protection authorities within the EU that is causing problems for businesses that are doing, you know, work across the—across the EU, different jurisdictions.

But also there's the potential, and this is, I think, relevant for us here, that there's overlap between the AI Act and the GDPR. And in some cases, those areas of overlap are going to need to get resolved one way or another, but it's causing some confusion.

Senator BLACKBURN. And digital marketing, and digital services, and some other—the overlap there.

Let me, I want to go to the data minimization issue. And again, just down the line. Mr. Lee, starting with you, what is your opinion of data minimization as a security principle in this debate?

Mr. LEE. I think it has to be integral.

Senator BLACKBURN. OK.

Mr. LEE. If we're going to reduce identity crimes, we're going to have fewer victims, we have to reduce the supply. Of data—

Senator BLACKBURN. Right.

Mr. LEE.—that can be abused by individuals if it's stolen, or even if it's just accidentally exposed. If you don't have it, you can't expose it, you can't—

Senator BLACKBURN. So you tie the two.

Mr. LEE. I do.

Senator BLACKBURN. Yes. OK. As you said, data breaches are the fuel. So that ties in.

Mr. Kaplan.

Mr. KAPLAN. Senator, from a macro perspective, I think data minimization is an increasing useful principle, especially in lessening the attack surface, particularly for those companies that are doing business with consumer-focused data. To that end, that's also where we think that, you know, legitimate and broad—not broad, but targeted permissible purposes like protecting the information, can be critical. But minimization can be an important tool.

Senator BLACKBURN. So you would segment it?

Mr. KAPLAN. Correct.

Senator BLACKBURN. OK.

Mr. Trivedi.

Mr. TRIVEDI. Thank you, Senator. I would say data minimization is an essential part of data security safeguards. Central to it, for the reasons that other witnesses have highlighted as well, which is to say, the attack surface is lessened when you sort of are intentional about collecting only what you need. You can't—again, you can't exfiltrate or hack what isn't there in the first place.

Senator BLACKBURN. All right.

Mr. Parker.

Mr. PARKER. Yes, I would say there's a—I mean, there is a bit of a difference between data minimization as an operational principle and a policy principle. So certainly from an operational standpoint, you know, this definitely plays a big role in data security. From a policy perspective, I know there's, you know, the overall approach of having a set number of permissible purposes for collecting and processing data. It certainly could work.

I know there are some questions out there about, what about future-proofing this. So that in the future, is that going to be too narrow? Do they cover what they need to now? Those are all legitimate questions, but certainly an interesting approach.

Senator BLACKBURN. Great. Can I ask—

Senator HICKENLOOPER. Sure.

Senator BLACKBURN. Oh, Peter's here, so I didn't see him. Go ahead and go to him. I've got another question I want to ask.

Senator HICKENLOOPER. And I've got Senator Klobuchar on as well.

Senator BLACKBURN. OK.

Senator HICKENLOOPER. Do you want to ask a particular question?

Senator BLACKBURN. I do. I wanted to talk about China. Because we just enacted legislation to force ByteDance to divest from TikTok. And the data security threat from China is broader than just TikTok. And a more holistic approach, rather than playing Whack-A-Mole is required on this. The problem goes beyond apps. And we know that China is using drones and cranes and potentially routers to spy on Americans.

So how should Congress approach the broader data security threat from China? And what do you see as a good policy solution to this? Mr. Lee.

Mr. LEE. I'm just a humble victim's advocate, but we do have to recognize that nation states, maybe not for the same reason as pro-

fessional criminals, they want the information, and it's important that it is protected from whomever wants to misuse it, for whatever reason they want to use it.

China is certainly a nation state that has great capabilities. We know that they have a lot of data about individuals for intel purposes. We have to assume there are other countries, friends and foes, that do the same.

So an approach for data protection needs to be universal in its approach to whomever is acquiring the information.

Senator BLACKBURN. Mr. Kaplan.

Mr. KAPLAN. Senator, yes. The threat from China is something that we are tracking every day on a regular basis, both the threat with exfiltrating information to China, but also other malign nation states that are looking to leverage sort of data within the United States.

As a cybersecurity company, we're principally focused on the security of the networks and information systems upon which that data relies. So broader policy sort of questions about how to deal more holistically with a problem, may be outside of our purview.

To that end, we would encourage strong cyber protections with regard to those systems and encourage information sharing with the Federal Government like we enjoy and we regularly partner in—with regard to that threat.

Senator BLACKBURN. Mr. Trivedi.

Mr. TRIVEDI. Thank you for the question. I think you're importantly highlighting the ways in which data security and data protection have a national security dimension. We've been talking about consumer protection, which is vital. We've been talking about people's privacy.

But this is not all occurring just in the context of what's happening with our own borders. And as Mr. Kaplan mentioned, I think there are a number of nations in competition for one another's data, and there are costs to that.

I would say, to answer your question about the right policy approach, at the top of the list should be establishing a Federal data security and privacy protection standard. Right? That's—I think that's essential because it does all the things we've talked about, but also confers national security benefits on America as well.

Mr. PARKER. And certainly what was just mentioned is establishing that standard in the Federal privacy framework we're talking about would be—would go a long way to doing that.

Certainly, anything that's Internet-connected devices is a target for exploitation by nation state actors. So implementing—you know, certain encryption protocols in our industry, as I'm aware, is pretty important. Protecting those specific kind of devices.

And I say, though, as an additional side note, there has been also a large shift within our industry away from manufacturers in China, and sourcing equipment there, that could possibly have vulnerabilities. So I'd say especially in the commercial sector, it has been near—a near complete move away from those sources.

Senator HICKENLOOPER. Great. Thank you.

Senator Welch.

**STATEMENT OF HON. PETER WELCH,
U.S. SENATOR FROM VERMONT**

Senator WELCH. Thank you very much. It's good to be here. Senator Blackburn, it's always wonderful to see you continuing this pioneering work that you began when you were in the House.

And it has only gotten more complicated, actually. Let me ask you a few questions about the privacy issues for individuals, and then the cybersecurity that's essential for everyone.

I mean, as you know, about 72 percent of Americans believe there should be more regulation over what companies do with people's data; 67 percent, and I'm among the 67, report little to no understanding of how companies use their data. And 73 percent report that they believe they have little or no control over what companies do.

So there's a question about my data, citizens' data, and what companies do. Then there's the question about hacking into systems. And companies, tech companies have a high self interest in doing everything possible to protect against hacking, because it hurts them and their customers.

I mean, where's the difference in the responsibility for protecting the system from being hacked? And I hear you saying there should be a national standard.

And that national standard, what does that mean for small businesses that just don't have the financial wherewithal to be able to bear that burden? And how what those recommended protections, how they could be integrated affordably, organically, into systems that a small mom-and-pop business might deploy?

And I guess I'd start with you, Mr. Lee.

Mr. LEE. Thank you, Senator. Let's work backward. Particularly for small businesses, this concept of the risk assessment is very important.

Senator WELCH. That they have to do themselves?

Mr. LEE. That they would do themselves, because that's where they understand where the risk is. So if you're prescriptive, and "You say you must do X," but you have no risk of that ever happening, that is a waste of their time and their energy and their money.

But if you do a risk assessment, so you understand exactly what you are facing in your unique business based on the information you have from your customers, then you are meeting that risk as it is today, and you're monitoring it—

Senator WELCH. OK.

Mr. LEE.—to see what you have to do to move it forward.

Senator WELCH. You know, I—let me push back a little bit. I'm just thinking, let's say it's a small record producer in Nashville, and they're a new startup. I mean, for that person in business to be talking to the customers about what they need, and then being able to make the decisions to deploy, that requires a level of sophistication that may not be the level of sophistication required to be a good record producer.

I mean, you know, I have a—or you're a small law firm, let's say. You know? I was in a law firm with four lawyers. It was pretty smart—small. We didn't have the demands or the capacity to do what the major Wall Street firms do.

So what you're describing as a step that we should take seems out of reach to me for the millions of small businesses we have. It seems to me that—this should be just available, baked into what it is you buy.

Mr. LEE. I guess I would view that that's actually the foundational step. It's—the one-size-fits-all approach, which we have taken heretofore is what burdens small businesses. But when you take a tailored approach where it's specific to their business and specific to their data, then you don't have to do things which you know you're never going to implement.

Senator WELCH. So no, that makes sense. But what's the expense associated with that?

Mr. LEE. Well, there—it depends on which tool you're using. If you—

Senator WELCH. Give me a ballpark. I mean, I'm worried about the small businesses having to deal with these massive impacts on their small business.

Mr. LEE. As a—you know, we've got representatives of the world's largest, you know, cybersecurity organization, but there are small, managed services providers that that's what they do. There's—I'm sure, hundreds of them, even in the Nashville area. In every city, there are people who do that.

I'll let you respond—

Senator WELCH. OK. Mr. Parker thinks—you know, you mentioned future-proofing, which makes a lot of sense to me. But one of the things that I've found frustrating as a member of the House and now in the Senate is, we can't keep up with all the changes and all the methodologies by which there is hacking. And even those who are far more expert in Congress on technology issues, I don't think, can keep up with it.

Senator Bennett and I think that we—the time has come where we actually need an agency, a digital commission, much like, say, the FTC or the FCC, that is properly staffed, properly resourced, and has the capacity to keep up.

Because if it's a one-off bill that's dealing with problem A or problem B, it's a very cumbersome and difficult process to get it done in a timely way through Congress.

Do you have any thoughts on the wisdom of having such an entity that would have as its ongoing challenge protecting privacy and—in considering other issues related to tech?

Mr. PARKER. Yes, I mean, so that's a great question. And I apologize, I don't have a great answer, but I know that the—obviously, the state of California has done something like that, having a privacy agency.

And so I know the issue has been discussed here as far as creating something like that. I know there's probably the opinion that most of the—that we have existing agencies are playing that role, but I understand what you're saying. I know that it's definitely bifurcated the way it is currently.

Senator WELCH. Well, Mr. Trivedi, you mentioned there should be a national standard? Right?

Mr. TRIVEDI. Yes. Yes, I did.

Senator WELCH. That makes sense to me. Who determines what that national standard is?

Mr. TRIVEDI. Well, I think that legislation would emerge from a number of stakeholders working together. But I would emphasize that it should be both strong and flexible. To your point about how smaller businesses are able to comply, we cannot expect, you know, a small record store, to your point, collecting potentially far less digital data than, you know, a large tech company, to meet the standard.

Senator WELCH. Well, what would a national standard look like? And “strong and flexible” makes a lot of sense to me. So what you’re saying, I agree with. But I’m trying to think about the practical way (a) to define it, (b) to implement it, (c) to change it. And this—sitting up here, I know that’s a tough ask for the folks in this job who are determined to do the best they possibly can. So do your best to answer that question.

Mr. TRIVEDI. Sure. Thank you, senator. It’s a very good question. I mean, I think there are some—some best practices I listed out as near-universal, that would apply.

So for example, even small businesses can think about and implement access controls to make sure employers who don’t need certain data can’t access it. They can, you know, engage in data minimization relevant to their—or relative to their capacity, which is to say, think hard about what they really need, and what they don’t need, they shouldn’t keep, because it’s also a risk to them. And it’s—

Senator WELCH. No, but we have to make—the legislation has to determine that. It’s not like you’re asking the individual to determine that. Right?

Mr. TRIVEDI. That’s right. I think—I think legislation should establish sort of a strong set of practices, but that there should, of course, be flexibility in how businesses of varying sizes comply with it. But there should be some basic requirements that are common.

Senator WELCH. So do you have a template of what it is you think Congress should pass?

Mr. TRIVEDI. Well, I think we’ve seen some credible bipartisan proposals. I think there’s good progress being made via the discussion draft of the American Privacy Rights Act.

Senator WELCH. Mm-hmm.

Mr. TRIVEDI. I do think that is a very promising proposal on the table today.

But in terms of a template specifically for how small businesses can operate, I think that’s something that we could get back to you on and think more about.

Senator WELCH. All right, thank you.

I yield back.

Senator HICKENLOOPER. Thank you.

Now we have by remote, Senator Klobuchar.

**STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA**

Senator KLOBUCHAR. Thank you very much, Mr. Chair. Thank you to the witnesses.

I’ll just start out by generally saying that we need a national privacy law that creates rule of the road. I support, after reviewing it, Senator Cantwell’s discussion draft of the American Privacy

Rights Act. I strongly believe that consumers should have access and control over how their personal data is being used.

Mr. Trivedi, do you agree that consumers should have the ability to access their data and control how it is used by companies?

Mr. TRIVEDI. I do, Senator. Thank you. I think access and control rights are very important for consumers.

Senator KLOBUCHAR. OK, thank you.

Mr. Lee? And I'm having trouble hearing it—I'll just try my best here.

Mr. Lee, we also need to educate Americans on how to identify and react to cyber threats. We know there are phishing schemes going on. Senator Thune and I have introduced the American Cybersecurity Literacy Act to educate the public on cybersecurity risks by requiring NIST to conduct a cybersecurity literacy campaign.

Can you talk about the importance of educating Americans on how to identify and avoid cybersecurity threats?

Mr. LEE. Well, education is a key to so many different things, and particularly in this case, it is a part and parcel of keeping people safe.

One of the things that we learn from talking to victims every day is they are very curious about how to make sure it doesn't happen to them again.

So having a comprehensive approach that is led by the Federal Government would be very helpful, because we overall—identity crime victims don't get a lot of support anyway, because a lot of times people think of them as victimless crimes. And trying to avoid that crime is even more difficult.

So education is going to be a key part of making sure that we are keeping people safe in this increasingly dangerous cyber world.

Senator KLOBUCHAR. Agree.

Mr. Kaplan, in just the past 5 months, we've seen significant data security breaches. Obviously United Health Group, AT&T, Microsoft. Because these companies maintain large amounts of data on huge swaths of the population, hacks often can affect tens of millions of people.

In your testimony, you noted that large companies have twice the number of systems exposed on the Internet than what they were monitoring. What complications to protecting consumer data arise from simply holding such vast amounts of it?

Mr. KAPLAN. Thank you for that question, Senator. Yes. Holding that vast amount of data just increases sort of your attack surface and your vulnerability, and makes you a more likely target of sort of the malign threat actors and nation states that are looking to sort of divine and exploit and pull out that data to make strategic use of it.

With regard to the attack surface, this was one of the basic cyber principles that we also talked about. It's understanding what your Internet-exposed attack surface looks like, understanding how many of the portals into your system are open to the public Internet, and having visibility into existing vulnerabilities, misconfigurations, you know, not updated pieces of equipment or software that are exposed to the open Internet, that just give those malign actors entree into the system.

So having visibility into the ecosystem and what your attack surface looks like to the attacker, we think, is a critical piece of securing your infrastructure. That, combined—

Senator KLOBUCHAR. Mm-hmm. Can—

Mr. KAPLAN.—with knowing what your data is, is all a critical element of maintaining—

Senator KLOBUCHAR. Yes. You—

Mr. KAPLAN.—customer confidence.

Senator KLOBUCHAR. You also noted in your testimony that the United Healthcare chain data breach is likely to be the largest supply chain breach of this—Mr. Lee—the largest supply chain attack in history, because of how many organizations depend on Change to process insurance payments.

When an entire industry relies on only one or two digital supply chain providers that hold and process huge amounts of data, how does that affect the impact of a cyber attack?

Mr. LEE. It's—for a cybercriminal, it's a nirvana if you can find a supply chain. Rather than have to attack a series of companies one at a time, if you can find that one organization that has weak cybersecurity, but lots of data from not just one company, but all of their customers, all of the people they support, they are going to get massive amounts of data.

And we've seen—at the ITRC, we've seen a 2,600 percent increase in the number of organizations hit by supply chain attacks. Not just that they were attacked—you may only have 100 companies attacked last year, but you had 2,600 companies that were impacted by it. Their data was exposed.

So for a criminal, these things are incredibly profitable. And it's something that we—well, the whole topic of this conversation is, how can we bring these other organizations up to speed so you do not have that risk from vendors to the larger organization?

Senator KLOBUCHAR. Yes, I mean, we have been helping dozens and dozens of hospitals and pharmacies and other health care providers in our state to become whole and to be able to function ever since this data breach.

And clearly work has to be done here, so you have—you can't have all this data in one place, and then they don't have backup systems.

Is that—would that be one of your suggestions? What would be your suggestions to protect this data? And this will be my last question.

Mr. LEE. I mean, from a data protection standpoint—I mean, there's a lot to that, only one part of which would be backups.

You know, there are just so many parts of the healthcare supply chain. It has been the industry that is most attacked for the last 6 years running, because there are just so many different parts of it, so many members, you know, from mom-and-pop organizations all the way up to a United Healthcare.

So while there are key things that they need to be done, a big part of it is just making sure that everybody in that supply chain is aware they are a target.

Senator KLOBUCHAR. Yes.

Mr. LEE. They are at risk. And to act accordingly.

Senator KLOBUCHAR. Exactly. OK. Thank you very much. Thanks everyone. Appreciate it.

Senator HICKENLOOPER. Thank you, Senator.

I still got some questions, and I think there are one or two people might be on their way here. So I'll indulge myself.

Mr. Parker—and I don't want to get you in trouble with any of your members in any way. But you know, the requirements for reporting a breach, whether it's ransomware or phishing or whatever it is, there are really—the penalties. Unless someone pays a ransom, the penalties so far don't appear to be significant in almost all cases.

Does there need to be some sort of an incentive or some way to reward some of the smaller breaches that are happening more frequently, that don't get the attention, and yet are, as I'm sure you're aware, costing us tens of hundreds of millions of dollars as a country?

Is that—I mean, how—within the framework of your membership, how do we get everyone eager to make sure that they report each incident?

Mr. PARKER. You know, that's a great question. I know—it has been a little while since I looked at this. I know every—I think every state has a law and—or a breach notification, they're different in some ways. Some have a private right of action applied to them. I think it—

Senator HICKENLOOPER. First—

Mr. PARKER.—definitely would—

Senator HICKENLOOPER.—first to have some of those requirements as well. But there's just not a heavy hand. It's fairly light.

Mr. PARKER. I mean, I know that some—I know—yes, the other witnesses may have a better idea here, but you know, certainly something should be a priority for the AGs that are enforcing these rules.

Senator HICKENLOOPER. Right. But again, they need—they'll need some penalty or there needs to be some incentive, some way of moving people. Anybody else want to comment on that? You know, don't feel the obligation, because I have more questions.

Mr. LEE. Oh, I've got comments. To your point, it took from 2003 until 2018 to get all 50 states, the territories, and the District of Columbia, to have a data breach law. And they are all different. They all have different triggers of what constitutes a breach. They all have different requirements for what is in a data breach notice.

And in every instance, it is the organization that has lost control of the data that gets to decide if there is a notice. Oregon will allow a consultation with law enforcement. But other than that, the organization makes the determination.

Where you live determines how much information you have, if you have any information, and what resources are made available to you. So when we talk about national standards, that's why we mentioned data breach notifications have to be part of that, because those are both education opportunities for the individuals, and they're opportunities to make sure that we don't have repeat occurrences.

Senator HICKENLOOPER. Absolutely.

Anyone else? You've all referred to at one point or another—I don't know whether there's a certain amount of irony in some of the comments, but the swiftness of response. Would you all agree that swiftness needs to be a goal, something that we should find ways, both within government but also within the business community, of accelerating responses and making sure that swiftness is—swiftness becomes an important factor.

Start with Mr. Parker, we'll go up this way just for a change of direction.

Mr. PARKER. Absolutely agree with that.

Mr. TRIVEDI. Yes. I think both on the cybersecurity incident response side, as well as on the pace at which we should move on data security and privacy legislation, swiftness is essential.

Senator HICKENLOOPER. Say that louder when you say that. Just—no, I'm just kidding. We want it to fill the room.

Mr. KAPLAN. Senator, swiftness when responding to a cyber incident is critically important.

One of the things that we've seen from Palo Alto Networks is the average incident response time for companies, as recently as 2021, was 44 days that it would take companies to address a cyber incident when it occurred. And it was 44 days till they started seeing data exfiltrated from those attackers.

We've seen that exfiltration timeline decrease to just days and hours. And if you take that in context with the average time that it takes for a company to respond to a cyber incident and mitigate it, is 6 days? If attackers are starting to exfiltrate data in one day, in just a handful of hours, you're losing data. So swiftness is a critical aspect.

Senator HICKENLOOPER. All right. Absolutely. Mr. Lee.

Mr. LEE. I agree.

Senator HICKENLOOPER. Great. Thank you. And I might have one more question.

First, I'm going to turn to Senator Budd.

**STATEMENT OF HON. TED BUDD,
U.S. SENATOR FROM NORTH CAROLINA**

Senator BUDD. Thank you, Mr. Chairman.

And again, thank you all for being here today. So much commerce, business work, and social interaction now takes place online, as you all know, and there's a large volume of sensitive data that goes into those online interactions. In many ways, that data has become the lifeblood of the digital economy, connecting small businesses with customers and improving online services.

So I know this firsthand as a small business owner who has run digital advertising campaigns myself.

I also know that the majority of businesses take data security extremely seriously. Burdening customers with what may feel like arbitrary, excessive, or overly sensitive personal information disclosures is a poor way to instill customer trust. And protecting against devastating breaches, it's a must.

Mr. Parker, you mentioned how important uniform standards and laws are to the Security Industry Association members. Is there an example that you could share where conflicting laws be-

tween states have reduced business opportunities for any member of companies?

Mr. PARKER. Sure. Absolutely.

So the kind of prime example of this is the Illinois Biometric Data Privacy Law, known as BIPA, where it was formulated, I think, more than 15 years ago, when that technology was in its infancy. A lot of misunderstandings about it.

But it's certainly—because of the way it was structured and the private right of action attached, it has created a sue-and-settle environment where there's tremendous litigation risk in fielding the technologies, even if they're deemed to be compliant.

And so, as a result, there are a number of our member companies who do not actually offer their products to customers in Illinois anymore, because of what's happened with that.

Senator BUDD. Any particular products that you can recall?

Mr. PARKER. Well, you know, there's—within biometrics, there are many different types of products. But just to give you an idea, 88 percent of the lawsuits under that law had been on—regarding biometric time clocks. Basically a way to authenticate your identity for punching in and out of work. No allegations that harm actually occurred to anyone. There was some, you know, misstep in the collecting consent and things like that that were found, and that was a basis for class action lawsuits.

And that's—things like that, even—it's—even though it's not in some products, certainly in the security area, cannot even be filled with there under the rules. But in other cases, you know, products like that, some people are just—say, forget it. We're not going to even bother.

Senator BUDD. You know, the savings from those systems, I would know firsthand, and they save businesses money, they make them more competitive, allow them to pay employees more, hire more employees. So I see the challenge there.

Mr. Parker, can you speak to how uniform national requirements and legal liabilities would improve the ability of your member companies to protect personal data?

Mr. PARKER. Yes, so, I mean, I think having a national standard, you know, that fully preempts, you know, state and local laws and data privacy would definitely save on compliance costs. But it would also be better, you know, for the global competitiveness of our companies that can align what they're doing, you know, with other parts of the world as well, versus having people track what's going on in each individual states and what products can be offered where, and under what circumstances. So there's definitely a tremendous advantage of having a national framework and standard.

Senator BUDD. Thank you. You mentioned that the Security Industry Association encourages its members to implement resources like how to counter AI-driven cybersecurity threats to physical security products, just an example. So your members seeing criminals use AI in new ways?

Mr. PARKER. Yes, so one thing we're certainly—I was just talking to some of our cybersecurity experts in the industry about this. But one thing that's emerging is the ability to detect when video has been altered. And so security video is obviously very important to, you know, what we do and provide to customers.

But you want to make sure that that can't be manipulated by bad actors for fraudulent purposes, or maybe even further, some other criminal activity. And so there's definitely technology available that is verifying the authenticity of data that's stored and making sure it hasn't been altered. So that's one—that's one area.

Senator BUDD. Thank you. Thank the panel.

Chairman.

Senator HICKENLOOPER. Thank you, Senator.

OK, I'll be quick. I know you guys been here for a while. And you've—a couple of you already commented on this. But I just put in a fair amount of—our office put in a fair amount of work on the American Privacy Rights Act.

And you guys, it affects what we're talking about today. It is about security in addition to privacy. I think all of you have pointed out that there's a connection there that is inviolate.

What's your feelings—and we'll go right down the list on APRA in terms of, if you've got some constructive—something bothers you or constructive criticism, it's out with it. But if you, if you think we need to have a sense of urgency, a couple people have referred to quantum computing as it comes down the pike. If it isn't giving us a sense of urgency around these issues, then nothing will.

Anyway, start with you, Mr. Lee.

Mr. LEE. I do think there should be a sense of urgency just because of—we don't even have to get to quantum. You can just look at artificial intelligence, and just the efficiency and the depth and breadth that it's bringing to everything from creating malware to a phishing attack.

We're seeing more and more phishing attacks, which are very basic, that are letter-perfect, that fool even professionals, they are so good. Whereas, you know, a couple of years ago, everybody kind of go, yes, yes. There's only, you know, Bank of America isn't spelled with B-A-A-N-K. You can't do that anymore.

It is good, and it is getting better. You have—for the most sophisticated, you've got Deepfake video, you have voice cloning. You have risks that are primarily to businesses, but individuals will be the vehicle to get to the business attack.

So there is a sense of urgency. My watch-out on the Privacy Rights act would be, beware of the law of unintended consequences. As we talked about a little bit with data minimization, we still need data, and we need it for some very specific purposes, because it's used for anti-fraud. It's used for identity verification, to prevent identity crimes.

So in our zeal to protect consumers and give them access, we also have to be realistic that we still need some data.

Senator HICKENLOOPER. Thank you.

Mr. Kaplan.

Mr. KAPLAN. Senator, we're still evaluating APRA. We do think that this current version, there are some beneficial aspects, like specifically—

Senator HICKENLOOPER. Wait, so I started this with a sense of urgency. You're still evaluating, come on.

Mr. KAPLAN. Well, with a sense of urgency, and I can hit that. So what we've seen with regard to artificial intelligence, for example, is, you know, to echo what Mr. Lee said, is we have seen threat

actors leverage this to create really sophisticated spear-phishing attacks.

Senator Blackburn brought up quantum. Quantum threats—right now, there is a campaign of harvest now and decrypt later, where malign nation states are collecting data, even encrypted data, knowing that this day is coming, where they'll be able to decrypt it.

So the urgency is really, harden your systems now and secure your systems now, and secure your data now.

One of the beneficial aspects of APRA that we see is those strong permissible purposes for cybersecurity companies. Mr. Lee also talked about the uses of data. Both for our cyber defenses, but also in the artificial intelligence.

And just a quick stat, we leverage AI across our systems and capabilities, and we are able to detect 2.3 million unique attacks that weren't there the day before.

This is a process of continuous discovery, and we're able to leverage our security data and those AI tools to block 11.3 billion attacks per day.

And that's just one player, one company, in the cyber ecosystem. So the utility of this data, I think, is proven. And that's where sort of the flexibility of something like the permissible purposes and APRA are critical to securing everybody's data.

Senator HICKENLOOPER. Great, great.

Mr. Trivedi.

Mr. TRIVEDI. Thanks for the question, Senator. I think, you know, and we've said publicly that APRA includes some of the necessary pillars of sound privacy legislation. I won't list all of them, but I think it is germane to today's conversation. Strong data minimization principles, online civil rights protections, privacy rights for users to be able to view, correct, and opt out and delete their data, stop at sale or transfer, these are essential elements of data protection and consumer protection. And so we are heartened to see this credible proposal reemerge.

In terms of constructive areas to focus on, I think one of the areas of concern for us has been the scope of FCC preemption in APRA. We've seen with the recent announcement from the FCC fining wireless carriers, and the depth of their expertise and ability to act, to be a cop on the beat with respect to ISP privacy, Internet service provider privacy, I think that's essential.

And so we would focus on this issue not to have over-broad preemption of the FCC's ability to exercise long-standing expertise in their domain on privacy.

Senator HICKENLOOPER. Interesting. All right, thank you.

Mr. Parker.

Mr. PARKER. So just to speak to urgency from a policy perspective versus cybersecurity, you know, three years ago, there was one state that had their data privacy law, and now there are 19. So, I think there's definitely a window of opportunity to have a Federal standard. Many of those states that have acted since then have very similar frameworks, so.

But there is a potential, if they're different enough, that a 50-state patchwork laws can harm the economy. And so it's important to consider acting soon.

That said, we're still looking at the proposal and gathering input from members, but definitely applaud Chair Cantwell and Chair Rodgers for working to get to this place. And I would say that they're significant improvements over what we saw two years ago.

In one example in particular, we're pleased with the data minimization, permissible use purposes related to cybersecurity, and physical security, which we think are very well defined and well crafted.

But there are some other issues and questions, mainly, I think, that need to be addressed, you know, in moving forward.

I mentioned earlier how important it is to have strong preemption. We're definitely getting questions from members about whether what's in the proposal now is adequate enough to be truly the national standard that it's intended to be. So I think that needs a clear, you know, a clear answer.

And there are a few other kind of more detailed issues in the bill, but we're definitely still looking at it and providing input.

Senator HICKENLOOPER. OK, well, keep those cards and letters coming, as they say on TV—I guess they used to say on TV.

Appreciate all those comments about APRA. I think—I have a great sense of urgency on it, and I think that this is a wonderful time to work on something like data privacy on a bipartisan basis right before big election. But this should not be a partisan issue.

And I think we've seen a lot of bipartisan participation so far. But I'm hopeful that the people you all represent will continue to push with a sense of urgency this year to get this done. I think it's doable.

I think we're done here for today. But thank you all for your effort. Members can submit additional questions for the record until May 22. We thank you in advance for taking the chance to—taking the time to, and the chance, to answer those, provide responses hopefully by June 5.

And with that, I will adjourn.

[Whereupon, at 4 p.m., the hearing was adjourned.]

A P P E N D I X

MAIN STREET PRIVACY COALITION
May 7, 2024

Hon. MARIA CANTWELL,
Chair,
U.S. Senate Committee on Commerce,
Science & Transportation,
Washington, DC.

Hon. JOHN HICKENLOOPER,
Chair,
U.S. Senate Subcommittee on Consumer
Protection, Product Safety, and Data
Security,
Washington, DC.

Hon. TED CRUZ,
Ranking Member,
U.S. Senate Committee on Commerce,
Science & Transportation,
Washington, DC.

Hon. MARSHA BLACKBURN,
Ranking Member,
U.S. Senate Subcommittee on Consumer
Protection, Product Safety, and Data
Security,
Washington, DC.

RE: Hearing on “Strengthening Data Security to Protect Consumers” on May 8,
2024

Dear Chair Cantwell, Ranking Member Cruz, Chair Hickenlooper, and Ranking
Member Blackburn:

The Main Street Privacy Coalition (MSPC) appreciates your holding a subcommittee hearing on May 8 and the opportunity to share our initial views on the discussion draft of the American Privacy Rights Act (APRA). MSPC supports the goal of establishing a national privacy and data security law that applies equivalently to all businesses handling consumers’ information and avoids potentially unintended consequences that would have disproportionate impacts on Main Street businesses and, in turn, negatively impact consumers and the American economy.

The House Energy and Commerce Committee’s efforts last Congress on the American Data Privacy and Protection Act (ADPPA) included, in some instances, ways to address concerns that had long been difficult to reconcile. In some specific provisions affecting our members, such as preserving customer loyalty plans, service provider requirements, and the treatment of franchise businesses, however, the APRA significantly departs from the successful compromises achieved in the consideration of the ADPPA. We look forward to working collaboratively this year with you and your colleagues on the Senate Commerce Committee to address the issues outlined below with the ultimate goal of enacting privacy legislation that establishes a single, uniform national privacy law.

MSPC firmly believes that consumers across the country should be empowered to control their personal data. Having data privacy and security laws that create clear protections for Americans while allowing our members’ businesses to serve their customers in the ways they have come to rely upon is a key goal. Achieving that goal, however, has been elusive. One of the challenges central to the Committee’s legislative effort is that the overwhelming focus on the data practices of so-called “big tech” companies can obscure the reality that data privacy laws also apply to, and must work for, Main Street businesses whose employees directly serve Americans in their daily lives.

The MSPC is comprised of 20 national trade associations that together represent more than a million American businesses—a broad array of companies that line America’s Main Streets¹ and interact with consumers day in and day out. From retailers to REALTORS®, hotels to home builders, grocery stores to restaurants, gas stations to travel plazas, and self-storage to convenience stores, including franchise establishments, the businesses represented by MSPC member associations can be

¹The Main Street Privacy Coalition website and member list may be accessed at: <https://mainstreetprivacy.com>.

found in every town, city, and state, providing jobs, supporting our economy, and serving Americans as a vital part of their communities.

Collectively, the industries that MSPC members represent directly employ approximately 34 million Americans and constitute over one-fifth of the U.S. economy by contributing \$4.5 trillion (or 21.8 percent) to the U.S. gross domestic product (GDP). Our success depends on maintaining *trusted* relationships with our customers and clients: trust that goods and services we provide are high quality and offered at competitive prices; and trust that information customers provide to us while we are serving them is kept secure and used responsibly. For these reasons, our associations have been actively engaged for many years with policymakers on data privacy legislation and regulations.

Six Principles for Effective Federal Privacy Legislation

Main Street businesses have no higher priority than earning and preserving trusted relationships with their customers, including by protecting and responsibly using the personal data that customers share with them. As policymakers consider the APRA and other legislative solutions to address data privacy concerns, our coalition urges adoption of legislation meeting the following core principles to ensure a comprehensive and effective national privacy law:

- *Establish a Uniform National Privacy Law:* The United States should have a sensible Federal framework for data privacy legislation that benefits consumers and businesses alike by ensuring that consumers' personal data is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws with a set of Federal rules for all businesses handling consumers' personal data is necessary to achieve the important public policy goal of establishing a single, uniform national privacy law.
- *Protect Consumers Comprehensively with Equivalent Standards for All Businesses:* To protect consumers comprehensively, Federal data privacy frameworks should apply requirements to all industries that handle personal data and not place a disproportionate burden on certain sectors of the economy while simultaneously alleviating other sectors from providing equal protection of consumer data. An equivalent data privacy standard should apply, regardless of whether a business directly collected data from a consumer or obtained it in a business-to-business transaction.
- *Create Statutory Obligations (Not Contractual Requirements) for All Entities that Handle Consumers' Data:* Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts. Service providers and third parties must have statutory obligations like all other entities to ensure their compliance with a Federal privacy framework, particularly when offering data processing, transmission, storage, or other services to tens of thousands of Main Street businesses.
- *Preserve Customer Loyalty Rewards and Benefits:* Any Federal data privacy framework should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships and set the terms of those relationships. Legislation should include safe harbors to ensure that consumers can purchase, or otherwise obtain, the goods and services they want by taking advantage of benefits, incentives, or enhanced services they earn from being loyal customers, even if other customers choose not to engage in such loyalty programs.
- *Require Transparency and Customer Choice for All Businesses:* Consumers deserve to know the categories of personal data businesses collect, how it is generally used to serve them, and the choices they have regarding those uses. These policies should be clearly disclosed in company privacy policies and readily accessible to consumers. These transparency and choice obligations should apply to *all* businesses handling consumers' personal data, including service providers, third parties, and financial services businesses.
- *Hold Businesses Accountable for their Own Actions:* Privacy legislation should not include terms that potentially expose businesses, including contractors and franchisees, to liability for the actions or noncompliance of a business partner. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability for other businesses that do not fulfill their own obligations under a Federal privacy law.

Main Street Privacy Coalition Views on the APRA Discussion Draft

We appreciate Chair Cantwell's efforts to develop the APRA discussion draft with House Energy and Commerce Chair Rodgers, however, we have initial concerns that the bill, as drafted, disproportionately and negatively impacts the industry sectors MSPC member associations represent. We appreciate the opportunity to work constructively with Senate Commerce Committee members and their staff to address the potential unintended consequences of new language in the APRA prior to its introduction and advancement in Committee markups, consistent with our coalition's history of productive dialogue on past legislation, such as the ADPPA.

1. *Preemption of State Law:* We appreciate the Senate Commerce Committee's past efforts to develop preemptive legislation that would establish a single, uniform national privacy law benefitting consumers and businesses alike by ensuring privacy protections are the same regardless of the State in which a consumer resides or a business is located. This is necessary to address the increasing patchwork of newly enacted state privacy laws that conflict and threaten the ability to provide comprehensive and uniform privacy protections to all Americans. Despite the underlying goal of preempting state laws in past committee legislation, we are concerned the APRA's current preemption provision is unlikely to withstand anticipated legal challenges in Federal court, potentially leaving States free to continue adopting privacy laws that would leave American consumers with different rights depending on where they live and would saddle Main Street businesses with compliance burdens exceeding the Federal standards set by Congress. We therefore urge the Committee to modify the APRA's preemption provision to meet the standards the Supreme Court has consistently ruled sufficient to create a preemptive Federal law. For instance, the APRA could avoid using a general rule that necessitates pages of exceptions—a form Federal courts have used as the basis to preserve similar State laws and frustrate Congressional intent—by instead specifying precisely which State laws are preempted by the APRA and making clear that future laws related to the specifically preempted laws would be similarly preempted. Such an approach would make the APRA much more likely to achieve its primary goal of creating a single, uniform national privacy law for all Americans.

2. *Private Rights of Action:* We understand the Committee's interest in authorizing private rights of action (PRA) in privacy legislation as a politically desirable element to advance a bipartisan privacy bill through Congress. Our member companies are concerned, however, with the APRA taking a leap that no State law has taken due to the technical complexity involved in entities achieving mistake-free compliance with data privacy laws, as well as Main Street companies' extensive experience with large volumes of demand letters threatening lawsuits with questionable legal claims that recently have proliferated under other areas of the law (*e.g.*, patent trolls and ADA website accessibility claims). More importantly, the APRA differs significantly from the ADPPA in that the APRA does not authorize the PRA to enforce the requirements for service providers or third parties under Section 11(a) through (c) because it limits the PRA's application only to covered entities under subsection 11(d). This is a surprising reversal of the ADPPA's application of the PRA in this section that disproportionately impacts Main Street businesses compared to their business partners. Under this PRA, private litigants' *only* recourse would be to sue the covered entities for failing to exercise reasonable judgment in selecting service providers or transferring data to third parties because they cannot sue the service providers or third parties directly for their own failures to comply with their Section 11 requirements. Further, the APRA does not offer a way for well-intentioned Main Street businesses to avoid litigation because it denies them any opportunity to cure *alleged* violations in claims for damages. All too often, provisions like this PRA permit potential litigants to exploit the Main Street business reality that obtaining legal representation to defend against alleged claims under a complex Federal law is too expensive. Those costs lead Main Street businesses to agree to settlements of even non-meritorious claims simply to avoid litigation, which has the compounding effect of making it more challenging for them to cover operational expenses and consequently costs Americans their jobs. Due to the complexity of achieving compliance, the disproportionate impact that the APRA would have on Main Street businesses, and their inability to avoid litigation for alleged violations, our members would prefer the Committee adopt an enforcement approach similar to what all State privacy laws have adopted as the most effective way to drive compliance with privacy laws: exclusive government agency enforcement against businesses after a 30-or 60-day cure period following agency notice of non-compliance. If that is not achievable politically, we urge the Committee to at least address the serious concerns raised above to ensure that America's Main Street businesses, their employees, and the customers they serve are not disproportionately impacted, com-

pared to other stakeholders, by the APRA's enforcement provisions as currently drafted.

3. Preserving Customer Loyalty Rewards and Benefits: It is clear that Americans overwhelmingly wish to continue participating in their customer loyalty programs that provide rewards, discounts and other benefits.² Additionally, the fifteen States that have passed comprehensive data privacy laws have all preserved loyalty program benefits for consumers by protecting the ability of businesses to continue offering better prices and services to customers who voluntarily participate in bona fide customer loyalty, club or rewards programs. Under the State privacy laws, loyalty plan clauses protect against construing the laws to prohibit (as discriminatory acts) the offering of discounted prices or other benefits to customers who voluntarily choose to participate in the plans, even if other customers choose not to participate in them. However, the APRA adds a new page of novel requirements for loyalty plans not seen in any State law. We have significant concerns that the draft text alters the carefully balanced language of the ADPPA that MSPC member associations previously supported after all stakeholders negotiated with the House Energy and Commerce Committee to ensure the ADPPA provision would preserve customer loyalty programs. For example, one of the current APRA requirements prohibits all transfers of *any* data in ways that exceed the bill's already established data transfer provisions that permit covered data transfers subject to an opt-out and sensitive covered data transfers subject to an opt-in, excluding permissible purposes. With these same APRA transfer provisions applying to covered entities offering loyalty programs, similar to how all State privacy laws' consumer rights and privileges apply to plan participants' data as well, it is unclear why the draft APRA would impose a new, more restrictive data-transfer regulation on loyalty programs that consumers must already opt into under the law. In its forthcoming consideration of the APRA, we urge the Committee to restore the previous balance achieved in the ADPPA's loyalty provision that mirrors the balance achieved in all enacted State laws. This is important to American consumers who wish to maintain their earned points, rewards and discounts, and is a critical need for Main Street businesses.

4. Service Provider and Third Party Requirements: Similar to the loyalty plan provisions, we are concerned that the APRA draft text of Section 11 alters the carefully achieved balance previously achieved in the ADPPA's service provider and third party requirements following stakeholder negotiations with House Energy and Commerce Committee staff over that bill's provisions. We appreciated that the ADPPA placed direct statutory obligations on service providers and third parties, and enforced these obligations with the same enforcement mechanisms as covered entities, to ensure their compliance with the law. However, we are concerned the draft APRA has altered the text of these requirements to remove both the direct statutory obligations as well as the enforcement mechanisms for service providers and third parties in ways that obviate their obligations to protect the consumer data received from covered entities. The APRA ultimately allows service providers and third parties to avoid liability by shifting it onto covered entities through subsection 11(d), the only subsection enforceable by private rights of action (as explained in point 2 above). As a result, under the APRA, nationwide and global service providers would not have the equivalent privacy requirements or enforcement provisions that apply to even the smallest Main Street businesses. To protect Americans' data privacy comprehensively, the APRA should ensure that businesses in all industry sectors face equivalent privacy requirements and enforcement of the law in order to close of any privacy loopholes that would leave consumers unprotected when their personal data is handled by a range of service providers and third-party businesses. For example, the APRA's critical data minimization obligations do not apply to service providers or third parties—these are privacy requirements that exist nowhere else in Federal privacy law and should be required of all businesses in the APRA.

5. Common Branding: One issue that the House Energy and Commerce Committee was able to resolve in their consideration of the ADPPA was an unintended consequence of holding franchisors and franchisees liable for each other's privacy law compliance. Many franchisees and franchisors share common branding but are distinct companies and should be treated as such. But the language of the APRA currently defines them as one single "covered entity" because the businesses operate with "common branding." That language had been used in the ADPPA at one time, but the bill sponsors recognized that it could lead to unintended consequences and took the "common branding" language out of the ADPPA before it was reported by

²According to a survey by Bond Brand Loyalty Inc., 79 percent of consumers say loyalty programs make them more likely to continue doing business with brands that offer them, and 32 percent of consumers strongly agree that a loyalty program makes their brand experience better. Bond Brand Loyalty Inc., *The Loyalty Report* (2019).

the House Energy and Commerce Committee in July 2022. The same should be done for the APRA in its definitions of “covered entity” and “third party” to avoid making broad groups of independent businesses jointly liable for one another’s behavior.

We appreciate your consideration of the views of Main Street businesses regarding the APRA as the Committee considers the discussion draft before it is introduced. This is not just a bill for “big tech” companies, and Main Street businesses will bear the full burden of complying with the regulatory obligations under the APRA. As you consider ways to improve the APRA prior to its introduction and advancement in the legislative process, the members of the MSPC appreciate your consideration of the above principles and concerns with the discussion draft, as well as our efforts to address these concerns prior to approving the APRA in Committee. We look forward to continuing our constructive dialogue with the Committee on these critical matters and welcome the opportunity to address each specific topic with your staff.

Sincerely,

The Main Street Privacy Coalition.

cc: Members of the U.S. Senate Committee on Commerce, Science & Transportation

CITIZENS FOR LEGAL REFORM
May 8, 2024

Hon. MARIA CANTWELL,
Chair,
U.S. Senate Committee on Commerce,
Science, and Transportation,

Hon. TED CRUZ,
Ranking Member,
U.S. Senate Committee on Commerce,
Science, and Transportation,

RE: Hearing entitled, “Strengthening Data Security to Protect Consumers”

Dear Chair Cantwell and Ranking Member Cruz:

Citizens for Legal Reform submits this testimony for the record of the above-referenced hearing held on May 8, 2024, by the Committee on Commerce, Science, & Transportation.

CLR is a 501(c)(4) organization that is dedicated to preserving the separation of powers and the accountability of the political branches at all levels of government in the United States. CLR opposes laws that delegate law enforcement power to litigants who are not actually injured by the people or organizations whom they are suing. CLR believes such laws are unconstitutional, eviscerate political accountability, and undermine the rule of law.

CLR applauds Chair Cantwell for her work in developing a legislative framework designed to safeguard the personal information of all Americans as reflected in the recently released discussion draft of the American Privacy Rights Act (ARPA). We understand that data and personal information are integral to the functioning of our economy but also can easily be exploited by bad actors. With that as background, while CLR appreciates the important policy objectives the APRA seeks to achieve, it believes only government officials, who are accountable to the people, should be charged with enforcing the law.

Consequently, as the Committee considers the ARPA, CLR urges you not to authorize individuals to function as private Attorneys General who may sue to enforce statutory violations even when they have not suffered any actual injury.

Constitutional and Policy Concerns with Citizen Enforcement of Public Laws

CLR appreciates the need for private plaintiffs to have the ability to sue to vindicate their rights when they have suffered actual harm by a person or entity who has acted illegally. But, as previously mentioned, there are significant constitutional and policy concerns with laws that rely in whole or in part on citizen enforcement.

First, there is a serious question about whether such enforcement mechanisms are constitutional. Under Article II of the United States Constitution, only the President has the power and responsibility to direct the actions of those who execute and enforce the law. The Vesting Clause makes clear that the “executive Power” vests exclusively in the President.¹ The Take Care Clause requires the President “take Care that the Laws be faithfully executed.”² Finally, the Appointments Clause provides for the President to appoint Officers of the United States, and provides that Congress may vest the appointment of “inferior Officers, as they think proper, in the

¹ U.S. Const. art. II, § 1.

² *Id.* art. II, § 3.

President alone, in the Courts of Law, or in the Heads of Departments.”³ Taken together, these three clauses make it clear that the power to enforce Federal law—and the accountability for enforcement decisions—lies solely with the Executive Branch.

In *Transunion LLC v. Ramirez*, the Supreme Court held that in order to have standing to sue, a plaintiff must show actual injury—a statutory violation alone is not enough.⁴ In that opinion, Justice Kavanaugh explained that, “[a] regime where Congress could freely authorize *unharmful* plaintiffs to sue defendants who violate Federal law not only would violate Article III but also would infringe on the Executive Branch’s Article II authority.”⁵

Second, private enforcement provisions eviscerate political accountability, which is a vital part of our representative democracy. Private parties empowered to enforce public laws have largely unchecked enforcement power because they are not accountable to voters or elected officials when they use a law for unintended purposes. Voters cannot vote them out of office, and legislators cannot meaningfully use standard tools like oversight hearings or appropriations to guide enforcement. Because of this, private enforcement provisions are often abused by financially or ideologically motivated private plaintiffs and their attorneys, who can enforce the law for any reason (*e.g.*, to force defendants into settlements in unmeritorious cases; because the defendant is a business competitor to the plaintiff; because the plaintiff disagrees with the enforcement priorities of the current Executive; or simply because the plaintiff dislikes the defendant) without accountability to anyone.

Third, laws and law enforcement must be predictable, and penalties must correlate to the severity of the statutory violation committed. Individuals and businesses complying with the law often rely on the executive’s interpretation of the law through, among other things, formal rulemaking and guidance documents. But when individuals are given broad authority to enforce general welfare statutes, they often will advance novel legal theories that, when successful, lead to unpredictable results. Moreover, citizen enforcement of public laws leaves no room for enforcement discretion, which is vital to just public policy and preserving liberty.⁶ To the individual suing, they are the hammer and every statutory violation—no matter how small—is a nail.

Problematic Private Rights of Action in the APRA

CLR appreciates the efforts of the Committee to limit the scope of the private rights of action in the APRA by targeting citizen enforcement to specific provisions of the Act.⁷ However, section 19 in the APRA discussion draft still creates an enforcement structure for certain provisions that would deputize the plaintiff’s bar and private citizens to act as roving, unaccountable “private attorneys general.”

Section 19 does not itself limit private actions to individuals who suffer an actual injury from an alleged violation of the APRA’s substantive terms. Although section 19 allows for recovery of “actual damages” for individuals who do suffer harm, there is no requirement in that section for any individual to prove actual damages to obtain other statutory remedies, including injunctive relief and—critically—attorney’s fees and other litigation costs. Any limitation must therefore come from the substantive sections themselves, and CLR finds three substantive provisions that private individuals may enforce in the discussion draft especially concerning because they impose no injury requirement.

Section 4(a) Notice Violations: Under this section, citizens would be permitted to sue to enforce requirements that each covered entity and service provider make “publicly available, in a clear, conspicuous, not misleading, easy-to-read, and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the covered entity or service provider’s data collection, processing, retention, and transfer activities.” Nothing in this section limits a violation—or the enforcement of a violation—to someone who was harmed by the lack of a publicly available notice of a privacy policy. Moreover, most, and arguably all, of the criteria set forth in section 4(a) for judging a privacy policy are subjective in nature and

³*Id.* art II, § 2.

⁴*Transunion LLC v. Ramirez*, 594 U.S. 413, 426–27 (2021).

⁵*Id.* at 429.

⁶*United States v. Texas*, 599 U.S. 670, 679–80 (2023) (“[T]he Executive Branch must prioritize its enforcement efforts [to] constantly react and adjust to the ever-shifting public-safety and public-welfare needs of the American people.”); *Heckler v. Chaney*, 470 U.S. 821, 832 (1985) (explaining decision to “refus[e] to institute proceedings” is part of the Executive Branch’s Article II powers); *In re Aiken*, 725 F.3d 255, 264 (D.C. Cir. 2013) (Kavanaugh, J.) (“One of the greatest unilateral powers a President possesses under the Constitution . . . is the power to protect individual liberty by essentially under-enforcing Federal statutes regulating private behavior.”).

⁷American Privacy Rights Act, § 19 (a)(1).

could invite litigation (*e.g.*, arguing a policy is not “easy-to-read”). To the extent the Federal Trade Commission issues clarifying regulations of what is required to be in a privacy policy, any mistaken omission of a particular requirement would expose the covered entity/service provider to a lawsuit. Accordingly, not only are citizens empowered to sue to enforce this section regardless of whether they incurred any actual harm, but the vagueness of the statutory terms would encourage unscrupulous attorneys and plaintiffs to seek out marginal violations and pressure settlements.

Section 11(d) Due Diligence Violations: Citizen enforcement also would be permitted to ensure that a covered entity exercises reasonable due diligence (1) in selecting a service provider and (2) deciding to transfer covered data to a third party. Whether a covered entity acted with due diligence in selecting a service provider is subjective. An individual who has experienced no actual injury could nonetheless sue under this provision and allege lack of due diligence was used simply because the individual does not like the company who the covered entity chose to serve as the service provider or transfer data to. Moreover, the FTC would have up to two years after enactment to publish guidance regarding how a covered entity is to comply with this section. As before, an uninjured individual could sue under this provision asserting that the covered entity did not act with appropriate due diligence and is encouraged to do so given section 19’s attorneys’ fees provision.

Section 13(a) Civil Rights Enforcement: Finally, citizen enforcement is permitted to ensure a covered entity or service provider does not “collect, process, retain or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability.” While CLR appreciates the need to ensure that the civil rights of individuals are not violated, anti-discrimination statutes are not immune from enforcement actions by uninjured individuals. The Americans with Disabilities Act, for example, allows for citizen enforcement. Over the last three decades we have seen thousands of lawsuits filed by uninjured “tester” plaintiffs alleging business do not meet ADA accessibility standards and engaging in abusive sue-and-settle tactics.⁸

As the Committee and Congress consider this legislation, CLR recommends Congress ensure that only government officials, who are directly accountable to the people, are empowered to enforce the statute. To the extent a private right of action remains in the bill, it should be limited to those individuals who have suffered an actual injury.

Thank you for your consideration.

KAREN R. HARNED,
Executive Director.

U.S. CHAMBER OF COMMERCE
Washington, DC, May 9, 2024

Hon. JOHN HICKENLOOPER,
Chairman,
Subcommittee on Consumer Protection,
Product Safety and Data Security,
United States Senate.

Hon. MARSHA BLACKBURN,
Ranking Member,
Subcommittee on Consumer Protection,
Production Safety and Data Security,
United States Senate.

Dear Chairman Hickenlooper and Ranking Member Blackburn:

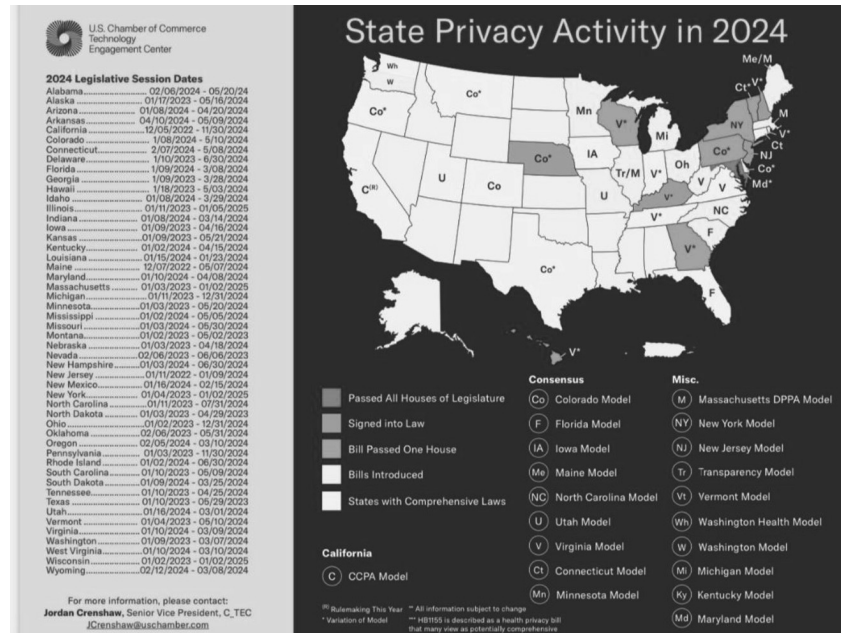
Thank you for the opportunity for the U.S. Chamber of Commerce (“Chamber”) to share our views regarding data minimization issues and our opposition to the draft American Privacy Rights Act (“APRA”) in the Subcommittee’s “Strengthening Data Security to Protect Consumers” hearing.

In its current form, APRA is deeply flawed and unworkable because it would fail to create a single national data privacy and security standard, would rely on the private trial bar for enforcement through private right of action provisions, and would impose unnecessary restrictions on goods and services that consumers enjoy.

⁸Minh Vu, Kristina Launey, & Susan Ryan, *ADA Title III Federal Lawsuits Numbers Are Down But Likely To Rebound in 2023*, Seyfarth Shaw (Feb. 14, 2023), bit.ly/42e1o5c; Bob Blum, *The Ninth Circuit Recently Undercut Defenses Against ADA ‘Serial Plaintiffs’*, DAILY J. (Feb. 17, 2023), bit.ly/3BZT3Ym; see also Brief of Amicus Curiae Center for Constitutional Responsibility in Support of Petitioner, *Acheson Hotels, LLC v. Laufer*, 22–429 (U.S.) (June 12, 2023), available at <https://tinyurl.com/CCRLauferAmicus> (discussing abusive litigation tactics present with ADA tester claims).

In the absence of such Federal privacy legislation, we have supported harmonized and workable proposals like the bipartisan Consensus Privacy Approach¹ in states like Virginia,² Texas,³ and Tennessee⁴ where more than 100 million Americans now enjoy privacy protections under a common framework.⁵

As drafted, APRA would reject full preemption and empower states to regulate beyond Federal standards.



I. Data Minimization

The Chamber recommends that APRA be revised to follow the Consensus Privacy Approach to data minimization to effectively protect consumers. Data minimization can be an important component of regulation to ensure the privacy and security of individuals, but overly broad, unnecessarily strict, or poorly crafted data minimization standards would impede innovation.

States that incorporated the Consensus Privacy Approach in law have enacted a balanced and workable data minimization standard. For example, states like Colorado, Tennessee, and Texas mandate that companies limit data collection to what is “adequate, relevant, and reasonably necessary” related to a disclosed or specified purpose.⁶

By contrast, APRA as drafted would limit all data collection and processing to “necessary, proportionate, and limit[ed] to provide or maintain” a specific product or service or consumer or anticipated communications.⁷ Although both the Consensus Privacy Approach and APRA have exceptions for certain practices like security, APRA would limit companies from collecting data that may be necessary for providing a service but can also have a societally beneficial purpose utilized by other

¹U.S. Chamber Model Privacy Legislation (February 13, 2019) available at https://www.uschamber.com/assets/documents/uscc_dataprivacymodel_legislation.pdf.

²Letter to Governor Northam available at <https://americaninnovators.com/wp-content/uploads/2022/08/Virginia-Data-Privacy-Act-Letter.pdf>.

³Letter to Texas House available at https://americaninnovators.com/wp-content/uploads/2023/04/State_HB4_TexasDataPrivacyandSecurityAct_TXHouse.pdf.

⁴Letter to Tennessee Senate available at https://americaninnovators.com/wp-content/uploads/2023/04/230417_State_BS73_TNPrivacy_TNSenate.pdf.

⁵Jordan Crenshaw, “What Congress Can Learn from the States on Data Privacy,” Real Clear Policy (January 2024) available at https://www.realclearpolicy.com/2024/01/30/what_congress_can_learn_from_the_states_on_data_privacy_1008521.html.

⁶See, e.g., Colo. Rev. Stat. § 6-1-1308(3); Tenn. Code Ann. § 47-18-3208(a)(1); Tex. Bus. & Com. Code Ann. § 541.101(1).

⁷American Privacy Rights Act Discussion Draft § 3(a).

companies. These secondary purposes include anti-fraud protections, Know Your Customer, and other web-based security applications, including those used by Federal programs to reduce theft of benefits and identity fraud. Secondary data sets have also enabled law enforcement to intervene and stop incidents of violence, human trafficking, and organized crime.⁸

II. APRA Fails to Create a Single National Privacy Standard

Congress should include in any Federal privacy legislation full preemption of state standards. A national privacy law without strong preemption would enable a state patchwork of laws that would be confusing to consumers and would potentially make it impossible for small businesses to comply.

A recent report highlighted that a national patchwork of privacy laws would cost the United States economy \$1 trillion and disproportionately impact small businesses with a \$200 billion economic burden.⁹ Many small businesses are worried that a patchwork of state laws will increase litigation and compliance costs.¹⁰

The APRA draft does not address concerns of the Chamber and other groups regarding of APRA's predecessor from the 117th Congress, the American Data Privacy and Protection Act. Although APRA's advocates express an intention to create "uniform national data privacy and security standard," the actual provisions of the draft provide only limited preemption and would allow states to pass more restrictive privacy laws. APRA only preempts "any law, regulation, rule, or requirement *covered by* [emphasis added] the provisions of this Act or a rule, regulation, or requirement promulgated under this Act."

According to a Congressional Research Service report, to provide the strongest preemption, Congress should use clearer and more forceful terms than "covering" or "covered by."¹¹ Congress should avoid merely preempting what a proposed bill is "covering" or "covered by," because such clauses are considered by the Supreme Court to be less restrictive on states than phrases like "related to."¹² According to the Supreme Court, "[c]overing" is a more restrictive term which indicates that preemption will lie only if the Federal regulations substantially subsume the subject matter of the relevant state law."¹³ A national privacy law that merely preempts what it "covers" and then provides for exceptions to that preemption would likely be taken by many as evidence that Congress has not intended to "substantially subsume" regulation.

The APRA draft would also create exceptions to preemption in the areas of consumer protection, health data, and remedies based on California's Consumer Privacy Act and highly abused lawsuits under the Illinois Biometric Privacy Law. These exceptions could easily be exploited in lawsuits and state legislatures to circumvent preemption in APRA.

There are better models. In recent years, legislation has been authored by both Republicans and Democrats that would provide strong preemption, including:

- H.R. 3388, the "SELF DRIVE Act," from the 115th Congress, which preempted broad categories of activities and passed the House by unanimous consent.
- H.R. 1816, the Information Transparency and Personal Data Control Act, from the 117th Congress, that provided: "No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard *related to* [emphasis added] the data privacy or associated activities of covered entities."¹⁴
- Financial Services Committee Chairman Patrick McHenry's "Data Privacy Act of 2023" draft from the current Congress, which provides that Federal legislation "supersedes any statute or rule of a State."¹⁵

⁸ Chamber Technology Engagement Center, "Data For Good: Promoting Safety, Health and Inclusion," (January 2020) available at https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf.

⁹ ITIF, "The Looming Cost of a Patchwork of State Privacy Laws," (January 2022) available at <https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/>.

¹⁰ U.S. Chamber "Empowering Small Business: The Impact of Technology on U.S. Small Business," (September 2023) available at <https://americaninnovators.com/wp-content/uploads/2023/09/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf>.

¹¹ Congressional Research Service "Federal Preemption: A Legal Primer," (May 2023) available at <https://crsreports.congress.gov/product/pdf/R/R45825>.

¹² *Id.* at 10.

¹³ *CSX Transportation, Inc. v. Easterwood*, 507 U.S. 663 (1993).

¹⁴ <https://www.congress.gov/bills/117/congress/house/bills/1816/text> (emphasis added).

¹⁵ https://financialservices.house.gov/uploadedfiles/glb_2023_xml_2.24_934.pdf.

III. APRA Fails by Providing a Private Right of Action

Comprehensive privacy legislation should leave enforcement to agencies like the Federal Trade Commission and state attorneys general, not the private trial bar. Such private rights of action would invite unwarranted lawsuits that would ultimately hamstring innovation and the viability of some innovators. Frivolous, non-harm-based litigation has been used in the past to extract costly settlements from companies, including small businesses. Private rights of action are ill-suited in privacy laws because they:¹⁶

- Undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who are best positioned to understand the complexities of compliance, promote innovation, and prevent and remediate harms.
- Entail inconsistent and dramatically varied, district-by-district court rulings. Agency enforcement can provide constructive, consistent decisions that shape privacy protections for all American consumers and provide structure for companies aiming to align their practices with existing and developing law.
- Are, when combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionately benefit plaintiffs' lawyers.
- Hinder innovation and consumer choice by the uncertain and pervasive threat of lawsuits, particularly for companies at the forefront of transformative new technologies.

Private rights of action would be particularly devastating for business under a privacy law that does not have a strong preemptive effect. Not only would states be able to continue passing their own laws, but individual judicial district precedent could also create further confusion and conflict.

IV. Substantive Concerns with APRA

- *Artificial Intelligence & Algorithms*—As drafted, Sections 13 and 14 of APRA would significantly impair America's lead in Artificial Intelligence. APRA as drafted would encourage lawsuits against companies that do not allow individuals to opt out of using basic technologies in any place of public accommodation, which could severely limit consumers' access to things like insurance, credit, employment opportunities, and other apps and services.
- *Small Business Impacts*—Small businesses would have to meet three elements of a vague test to determine if are exempt under the bill. Given APRA's private right of action provisions, small businesses would likely have to bear high litigation costs just to prove they are not covered by the bill. Even if a small business is not directly covered by the bill, we are concerned that the digital tools small businesses rely on could be threatened by other elements of APRA.
- *Digital Advertising*—The online advertising ecosystem is what enables Americans to enjoy the benefits of low-cost access to websites and apps. Unfortunately, as drafted APRA's data minimization, new FTC authorities to define what data is subject to opt-in consent, and universal opt-out for targeted advertising will threaten the contextual and personalized advertising that has driven U.S. Internet growth and innovation.
- *Data Broker Requirements*—While the Chamber does not take issue with a data broker registry, we are concerned that the bill's mass "Do Not Collect" requirements for data brokers would inhibit such important and beneficial uses as fraud prevention, small business marketing, healthcare, charitable contributions, and commercial credit and financing services.
- *Loyalty Program*—We are concerned that the APRA draft's prohibition on price and service discrimination could impair customer loyalty programs. Section 8(b)(a)(i)(IV) would require companies obtain "affirmative express consent for the transfer of any data collected in connection with a bona fide loyalty program." There is concern this provision would require consent every time data is transferred and would subject companies to private rights of action for inadvertent errors if consent is required every time. Such a requirement would have

¹⁶ U.S. Chamber Institute for Legal Reform, "Ill-Suited: Private Rights of Action and Privacy Claims," (July 2019) available at https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf.

a chilling effect on offering loyalty programs like hotel, restaurant, and retail programs consumers enjoy.

The Chamber opposes APRA in its current form. We stand ready with the Subcommittee and other members of Congress to enact meaningful and workable national privacy legislation.

Sincerely,

JORDAN CRENSHAW,
Senior Vice President,

Chamber Technology Engagement Center,
U.S. Chamber of Commerce.

cc: Committee on Commerce, Science, and Transportation

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
JAMES E. LEE

Cultural Change

Culture change is hard, even when organizations have the tools and resources necessary to implement change. This is also true with respect to creating a culture of data security.

Question 1. From your perspective, do you think U.S. companies are beginning to do a better job of adopting a culture of data security?

Answer. Yes and no.

Cybersecurity spending to prevent data compromises that expose personal information continues to increase overall and security teams are able to prevent or block the vast majority of attacks that lead to most security and data breaches. Even an organization as small as the ITRC is attacked hundreds of times each day, requiring constant improvements and investments to keep pace with threat actors—yet, improved security products and postures allow the successful defense of systems and data.

Increased investment in employee training, especially among small businesses, is also contributing to an improved environment for cybersecurity and data protection according to ITRC research and analysis of data breaches at SMBs. The overall number of preventable data compromises resulting from physical attacks as well as human and system errors have dropped significantly since 2018. Compromises from physical attacks have dropped from 13 percent (13 percent) of all compromises in 2018 to two percent (2 percent) today. Compromises from human and system errors have dropped from 23 percent (23 percent) to 19 percent (19 percent).¹

However, no sector and no industry is immune from attack and threat actors continue to successfully target organizations that are under-resourced, under-staffed, and rely extensively on legacy technology. Supply chains are especially vulnerable to attack and data breach statistics since 2018 show a dramatic rise in attacks against supply chains—2600 percent. The MoveIT Supply Chain Attack in 2023 is a classic example where 102 organizations were directly attacked, but the data of more than 1,270 organizations was compromised impacting an estimated 72M individuals. Likewise, the more recent attack against Change Healthcare involved a supply chain attack where 40 year-old technology was still the core of the company's network and facilitated the breach.

The patchwork of state and Federal laws and regulations that exist today have created the current environment. A fundamental shift toward enforceable minimum standards can address the gaps that exist today that allow threat actors to exploit weak security practices and victimize millions of U.S. residents each year.

Nowhere is this more evident than in the lack of a national standard for issuing data breach notices. Today, where you live determines if a compromise of personal information warrants a data breach notice and what, if any, information is shared with victims about the attack, the corrective actions taken, and protections & support provided to victims. Even state officials are not informed of data breaches in 16 states.

In 2023 the ITRC tracked an average of nine (9) new data breach notices each day compared to the 335 filed each day last year with data protection authorities in the European Union. Further, Federal court decisions since 2019 have resulted

¹The number of human and system errors would be nine percent (9 percent) today but for a recent rise in correspondence containing personally identifiable information (PII) being shared with employees or other individuals not authorized to receive the PII—i.e. someone attached a file containing PII to an e-mail that included people not authorized to receive the information. There is no indication data was shared with identity criminals in these compromises.

in only 32 percent (32 percent) of data breach notices filed in Q1 2024 containing information about the root cause of cyberattacks that led to data compromises.

Uniform minimum standards for data practices and security backed by risk assessments, audits, and strong enforcement actions can help elevate the practices, processes, and outcomes at all organizations that collect, process, and maintain personal and business data.

Question 2. What are best practices that can guide companies towards improved data security?

Answer. Significant improvement will require broad adoption across all sectors and industries of a variety of best practices—some technical and some practical—that will reduce the risk of personal information being compromised in data breaches and/or cyberattacks. These include the adoption of:

- *Data Minimization* practices to reduce the volume of information collected and/or retained which reduces the likelihood it could be compromised in a data breach.
- *Zero Trust* principles to require the verification of software and hardware before implementation and reverification when updated or modified.
- *Least Privilege Access* to give employees access only to information directly related to their jobs.
- *Security by Design / Privacy by Default* product design principles to ensure data and privacy protection are parts of the entire product lifecycle.
- *Regular Risk Assessments* to require cyber and data protections equal to or greater than the actual risks an organization faces; regularly scheduled risk assessments help ensure security programs address the ever-evolving threat landscape rather than the threats that existed when a security plan was originally developed or devote resources to “one size fits all” defenses that are not based on addressable risks.
- *Mandatory third-party audits* that ensure organizations comply with their own security policies/procedures as well as ensure the data protection program design is equal to the risk the entity faces.
- *Data Encryption in transit and at rest* will help ensure that if personal information is intercepted, exfiltrated or otherwise exposed, the data is useless without decryption keys.
- *DevSecOps* practices to link security outcomes to software development. Generally, software developers are not evaluated on the security of the code they write before it is put into production, resulting in significant dwell time between when threat actors begin their attack, when the attack is discovered, and when the flaw is ultimately patched. IBM reported in 2023 the mean time required to identify a breach was 204 days with an additional 73 days required to halt the attack and fix an underlying flaw.
- *Virtual Patching and Real-time Rule Application* reduces the time to patch and secure vulnerable enterprise applications from months to minutes. Independent researchers at Vanson Bourne reported in April 2024 that one-third of ransomware attacks were the result of a known but unpatched software flaws. Verizon analysis showed the number of global data breaches resulting from unpatched software increased 180 percent (180 percent) in 2023. Virtual Patching allows security teams to temporarily fix flawed code until a permanent patch can be applied when updating source code. Real-time Rules can be applied while an application runs, protecting enterprise software from Zero Day and other broad classes of attacks.

In addition, there are technologies that rise to the level of best practices that can also help improve data protection, including:

- *Biometric Verification* (not recognition) to help prove a person is who they claim to be since personal information used for ID purposes has been widely compromised in data breaches. Verification against a known source of truth—a photo in a DMV database, for example—with the applicant’s consent helps secure an individual’s identity and devalues the personal information stolen in a data breach that would otherwise be used to impersonate an individual.

Data Minimization

Data minimization—the principle that businesses should only collect the personal information they need and keep it only for as long as they need it—is where good data hygiene starts.

Just over a month ago, we learned from AT&T that the personal information of over 70 million of its American customers was released on the dark web. What is particularly concerning is that over 65 million of those consumers are not current AT&T account holders and haven't been since at least 2019. The sensitive data on the dark web social security numbers, account numbers, and passcodes.

This raises questions about why AT&T retained the information belonging to nearly 65 million Americans years after they stopped being AT&T Customers.

Question 1. What are the risks to consumers when companies hold on to data longer than they need to?

Answer. Maintaining excess data or personal information beyond its useful life creates a multitude of risks for the individuals who are the subject of the information as well as the organizations that hold the data. Static or near-static data such as SSNs, dates of birth, passports, state-issued driver's licenses or state IDs, are often misused in real identity fraud as well as synthetic identity fraud where identities are created from bits & pieces of real or imaginary data.

In 2023, the most reported types of identity misuse to the ITRC were Existing Account Takeover (52 percent) and New Account Creation (36 percent). Today, real but compromised identities are used to impersonate someone to open new bank accounts, take-over existing accounts, apply for state or Federal government benefits, secure loans, file tax returns, and obtain letter-perfect fake credentials that can be used to pass identity verification processes. Fake credentials with information of victims but with the photo and physical characteristics of the identity criminal are also used to evade law enforcement.

Information stolen in data breaches may circulate for years and the time to resolve any actual misuse of the information may also have a long tail. In many cases, the victims of these instances of identity fraud do not know their identities have been misused until months or even years later when they receive a notice from a creditor or government agency. Other victims learn of the misuse when they are denied a benefit or when an application for employment, insurance, or credit is rejected. Sixty-five percent (65 percent) of victims who reported their issues in 2022 to the ITRC listed their issues as "unresolved" as of August 2023.

The particular instance involving AT&T is another example of the ineffectiveness of state data breach notice laws which allow the organizations that have lost control of information to determine if a breach notice is required. The data in question first appeared in 2019 in a criminal identity forum where the information was listed as being AT&T account information. The company speculated the source of the data was a vendor with access to account information as the source of the breach and did not issue breach notices.

The same information was offered multiple times for sale subsequent to 2019 and each time AT&T denied being the source of the information. In early 2024 when the data was again offered to identity criminals, this time for free, AT&T acknowledged the information was related to past and current customers.

While the Federal Communications Commission and the Securities and Exchange Commission have recently strengthened the requirements for issuing security and data breach notices for telecommunications and publicly traded companies respectively, the vast majority of organizations that report data breaches are not covered by either agency's rules. In 2023, only 358 out of 3,205 data breaches (or 11 percent) were reported by public companies subject to Federal disclosure rules.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BEN RAY LUJÁN TO
JAMES E. LEE

Question. Please enumerate the cybersecurity risks that generative AI has introduced and share your recommendations for how Federal policymakers can design policies that mitigate these risks.

Answer. Hard statistics quantifying the increased identity risks associated with generative AI are rare. Anecdotally, the ITRC has received reports since generative AI reached the mass market in 2023 from victims and small businesses that support the analysis that generative AI is having several key impacts on cyberattacks and identity crimes. For example:

- Phishing attacks are more effective as generative AI has improved both the messaging and execution of phishing lures. No longer riddled with bad grammar, poor spelling, ill-designed graphics, and tone-deaf pitches, phishing e-mails and texts are now harder to spot and can fool even the most skilled cybersecurity professionals. The narrative they weave is far more compelling,

too, thanks to generative AI. The end result is more people believing phishing lures.

- Generative AI tools have allowed identity criminals to move from “Deep Fakes” that are expensive and labor intensive to “Cheap Fakes” that allow criminals with little to no tech skills to create voice clones and photo realistic facial clones for the price of a couple of cups of Starbucks coffee. These fakes are used to attempt to fool rudimentary verification tools to give criminals access to new or existing accounts or trick employees into taking a particular action such as paying a fake invoice.
- AI-designed cheap fakes are being used to attack individuals on an opportunistic basis, but the primary targets remain businesses—using the cloned voices of company executives and employees to prompt the payment of fake invoices or transfer of funds to fraudulent accounts.
- With access to troves of stolen identity data and openly shared personal information on social media platforms, identity criminals use generative AI tools to identify targets for various scams and identity fraud as well as refine the criminal pitch to make it more compelling to the intended victims.
- Cybersecurity researchers at the University of Illinois have proven it is possible to by-pass common generative AI security protocols allowing bad actors to create malware using generative AI that is designed to exploit software flaws based solely on the public notice of the vulnerability filed with NIST or MITRE.

While the ITRC generally does not lobby for or against any particular policy or legislative solution, we believe U.S. residents and organizations are at increased risk from the misuse of legitimate AI tools offered by legitimate developers. Many of those risks, however, can be addressed by the principles already under consideration in the APRA.

Operationalizing data minimization, risk assessments that envision a defense to AI-driven attacks, and audits that demonstrate the effectiveness or weaknesses of AI defenses—backed by strong enforcement regimes—are good examples of principles that would reduce the risks associated with the misuse of mainstream generative AI tools.

The greater risks to people and organizations, though, are from the malicious use of generative AI tools by identity criminals and Nation/States who do not “play by the rules.” In these cases, strong law enforcement and national security responses will be required.

Another area that warrants further consideration is the lack of user support for compromised social media accounts that could lead to large scale identity scams and mis- or disinformation using AI. Social Media Account Takeover (ATO) impacts 50 percent (50 percent) of victims of non-financial ATO, most of whom never regain access to their accounts according to ITRC surveys of individual and small business victims. With little to no support from the social media platforms, these compromised accounts often remain under the active control of an identity criminal and represent an on-going threat to other individuals who may be lured into a scam.

While there is no direct evidence at this time these attacks are being automated using AI, there is sufficient anecdotal evidence to warrant concern that threat actors could weaponize compromised accounts using malicious AI tools at scale. A bipartisan coalition of state attorneys general have recently contacted the major social media platforms seeking dialogue on the lack of responsiveness from platforms regarding ATO and the difficulty users face in reclaiming or shutting down compromised accounts. The ultimate answer may lie in a standard that addresses how social media platforms respond to ATO attacks and similar account compromises.

Finally, a comprehensive and sustained education program is needed that leverages the public, private and non-profit sectors to help individuals and small businesses avoid falling victim to AI-fueled scams, fraud, and dis- & misinformation campaigns. One example of a consumer education program is the partnership between the ITRC and the New Mexico Attorney General’s Office where identity crime victims can access expert advice about identity theft and fraud, free of charge, directly from the ITRC using a Live Chat link embedded in the AG’s website.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
SAM KAPLAN

Quantum Computing

Existing public-key encryption systems, which rely on math problems that are virtually unsolvable for conventional computers, can be quickly broken by quantum

computers which can perform such calculations exponentially faster than conventional computers.

Such computers capable of overcoming current encryption techniques are not yet available, but researchers warn that organizations need to start preparing now.

Already, cyber-criminals are stealing and storing encrypted data so they can one day use quantum computers to decrypt the data.

To address this threat, NIST is leading a multi-year effort to develop and standardize new “post-quantum” cryptographic algorithms to resist attacks from quantum computers.

Question 1. How are these programs going?

Answer. Many industry and government experts have been preparing for the challenge of encryption-breaking quantum computers for a long time. The U.S. National Institute of Standards and Technology (NIST) is soon expected to conclude a seven-year process, and publish the first set of Post-Quantum Cryptographic (PQC) algorithms, with the ultimate goal of establishing new, secure, quantum computer-resistant encryption standards. Upon their release, organizations will be able to begin validating whether their existing security technologies are interoperable with the newly selected PQC algorithms.

At Palo Alto Networks, we are committed to being a strategic partner to organizations on their journey towards quantum readiness. We have begun implementing quantum-resistant capabilities across our technologies, starting with a Post-Quantum VPN and new capability to discover PQC algorithm use within an organization’s network. We emphasize the importance of embracing several core principles that we see as essential capabilities of a comprehensive PQC security capabilities:

- Open Standards-Based: PQC security capabilities should be built on open standards, such as the cryptographic standards being developed by NIST, and not proprietary technologies.
- Integrated: PQC security capabilities should be fully integrated into existing cybersecurity technologies that organizations already know and trust.
- Scalable: PQC security capabilities should be able to be deployed in a tailored manner, commensurate with risk.
- Agile: PQC security capabilities must be capable of rapidly shifting to use different cryptographic algorithms seamlessly, with minimal operational disruption.

It is critical to not just talk about these core principles, but to demonstrate them technically in real world and test lab environments. Towards that end, we are honored to serve as a partner in NIST’s National Cybersecurity Center of Excellence (NCCoE) Migration to Post-Quantum Cryptography project. At the NCCoE, Palo Alto Networks partners with NIST, the NSA, CISA, and over thirty industry peers. The project provides a critical forum to demonstrate our latest technological innovations and our commitment to open-standards-based interoperability with the broader technology ecosystem.

The outcome of this public-private partnership will be a series of NIST Special Publications—blueprints to help organizations tackle common quantum security use cases, like conducting baseline cryptographic inventories, prioritizing which high value digital assets require PQC protections, and ultimately implementing validated PQC security solutions that demonstrate core attributes, like multi-vendor interoperability, crypto-agility and alignment to open standards.

Question 2. In your view, is quantum decryption something that we need to be concerned about?

Answer. Every day, the security of billions of global digital transactions, from e-mail and online banking to internet-connected medical devices, relies on a time-tested form of encryption called public key cryptography. This secures methods of identifying users, devices, and applications within a network, which is fundamental to authentication and confidentiality, and underpins a significant amount of today’s data sharing, data transfer, and transactions.

However, the arrival of encryption-breaking quantum computers (possibly within a decade) will undermine this foundational cryptographic underpinning of modern cybersecurity, resulting in decrypted and stolen secrets and intellectual property theft. Quantum decryption has been financially fueled by nation states seeking to use it as a potential geopolitical cyber tool.

As a *U.S. government advisory* warned, organizations everywhere should begin now to plan their transition to “Quantum Readiness” as a fundamental part of their security and business continuity strategies. Organizations should immediately take the following steps to kickstart their quantum readiness journeys: assign resources and build awareness; define responsibilities within the organization; develop an in-

ventory and priority list; evaluate, experiment, and test solutions to secure assets; and review, monitor, and refine policies.

We urge organizations to invest in quantum readiness, including the deployment of Post-Quantum VPN capabilities, *now* to prevent so-called “Harvest Now, Decrypt Later” attacks.

Privacy Enhancing Technologies

There are several techniques for keeping our data secure that fall under the term “Privacy Enhancing Technologies,” or PETs. PETs encompass many different technologies and techniques and can provide both data security and the ability for businesses to use data without accessing personally identifiable information about consumers.

Question 1. Without getting too deep into the weeds, can you describe these technologies and how they are used to secure our data?

Answer. At a high-level, PETs are capabilities that companies or organizations can use and deploy to protect the personal information they collect, while being able to simultaneously gather analytics or research from the data without having to access the actual personal information. General examples can include types of anonymization, encryption, or data masking. PETs can be helpful tools to protect personal data from unauthorized access or inadvertent data leaks.

Question 2. Do you agree that Congress can do more to incentivize the development and deployment of PETs?

Answer. PETs have the potential to help shrink the attack surface by limiting the amount of data that entities need for critical functions. It is important to study the efficacy and effectiveness of these tools to ensure any proposed policies or mandates would be complementary to cybersecurity efforts to protect privacy across the digital ecosystem.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO SAM KAPLAN

Question 1. What can the Federal government do to strengthen cybersecurity in smaller, rural health care facilities that have less resources to dedicate to cybersecurity protection?

Answer. Cybersecurity companies can help provide holistic and integrated platforms, backed by cutting-edge ML and AI technologies, that simplify complexity and streamline cybersecurity operations for resource-strapped organizations, helping to combat two of the largest hurdles: budget and human capital.

I mentioned six general recommendations in my written testimony to drive cyber resilience. All certainly apply to small businesses and rural healthcare facilities, but it is worth reinforcing two of them.

- 1). Ensure complete visibility of attack surfaces to help identify and mitigate vulnerabilities before they can be exploited. You can’t secure what you can’t see. It is critical to understand what you have exposed on the internet.
- 2). Maintain and test an incident response plan. Adversaries are simply too sophisticated for any entity to be caught flat footed.

There are also free resources available to help small businesses build cyber resilience. For example, CISA offers a number of free CyberHygiene tools. In October 2023, CISA published its “*Mitigation Guide: Healthcare and Public Health (HPH) Sector*,” which provides guidance on combating cyber threats in the healthcare and public health sector.

Question 2. In the hearing and within your written testimony, you describe the positive role that AI is playing in enabling swifter and stronger cybersecurity protection. Please enumerate the cybersecurity risks that generative AI has introduced and share your recommendations for how Federal policymakers can design policies that mitigate these risks.

Answer. Cyber adversaries are already leveraging AI to advance their tradecraft and will continue to do so going forward. For example, we see evidence that adversaries are using generative AI to enhance what we call social engineering attacks—phishing e-mails designed to lure users to “click the link.” Historically, these messages have been littered with poor grammar and typos, making their fraudulent nature relatively easy to detect, but they are becoming more accurate and therefore more believable. Adversaries are now able to generate flawless, mistake-free text, enabling click-through rates to skyrocket.

Additionally, bad actors are innovating with AI to accelerate and scale attacks and find new attack vectors. They can now execute numerous simultaneous attacks on one company across multiple vulnerabilities. Adversarial use of AI allows faster lateral movement within networks and more rapid weaponization of reconnaissance data. Going forward, there is the potential for a significant surge in malware variants as the cost of creating customized malware drops substantially.

These risks heighten the importance of leveraging AI and automation in threat detection and cyber defense. They also underscore the importance of safeguarding the entire lifecycle of an AI system, from data collection and model training to deployment and maintenance. These secure AI by design concepts encompass protecting data used for training AI models, ensuring the integrity of AI algorithms, and guarding against unauthorized access or tampering.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
PREM TRIVEDI

Data Minimization

Data minimization—the principle that businesses should only collect the personal information they need and keep it only for as long as they need it—is where good data hygiene starts.

Just over a month ago, we learned from AT&T that the personal information of over 70 million of its American customers was released on the dark web. What is particularly concerning is that over 65 million of those consumers are not current AT&T account holders and haven't been since at least 2019. The sensitive data on the dark web social security numbers, account numbers, and passcodes.

This raises questions about why AT&T retained the information belonging to nearly 65 million Americans years after they stopped being AT&T Customers.

Question 1. What does the AT&T breach tell us about data minimization?

Answer. As with many large-scale breaches, the AT&T breach powerfully underscores the need for data minimization throughout the data life cycle. Data should be minimized when it is collected, while it is being used, and retained only as long as it is needed.

Data that isn't collected in the first place cannot subsequently be stolen in a breach and released by hackers onto the dark web. Companies that minimize data collection will reduce their need to safeguard sensitive data like Social Security Numbers once breaches occur.¹ In addition, many companies are collecting so much data that they cannot identify where some breaches originate. Three years after a different data breach that occurred in August 2021,² AT&T still could not say exactly where that data set originated and whether or not it came from a third-party vendor.³ These data governance challenges also manifest in many companies' ability to appropriately minimize data use.

Companies also continue to demonstrate that they will not responsibly self-govern on data retention in the absence of data minimization requirements. More than 90 percent of the 70 million individuals impacted by the most recent AT&T data breach were no longer AT&T customers, but they still must confront the impact of their information being released and the very real threat of identity theft.⁴ AT&T's failure to delete at least some of this data through periodic reviews of its holdings drives home the inadequacy of its current data minimization practices. And AT&T is hardly the only company in this position.⁵

¹ AT&T Addresses Recent Data Set Released on the Dark Web, AT&T, Mar. 30, 2024, <https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html>.

² Millions of customers' data found on dark web in latest AT&T data breach, NPR, Mar. 30, 2024, <https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web>.

³ Zach Whittaker, AT&T won't say how its customers' data spilled online, TechCrunch, Mar. 22, 2024, <https://techcrunch.com/2024/03/22/att-customers-data-leak-online/>.

⁴ Consumer Sentinel Network | Data Book 2022, Federal Trade Commission, Feb. 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

⁵ Large-scale breaches in recent years have implicated a range of companies as diverse as First American Financial, Marriott, and Equifax. See, e.g., AJ Dellinger, *Understanding the First American Financial Data Leak: How Did It Happen and What Does It Mean?*, May 26, 2019, <https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=340923d7567f>; Marriott Announces Starwood Guest Reservation Database Security Incident, Nov. 30, 2018, <https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident>; Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, Jul. 22, 2019, FTC press release, <https://www.ftc.gov/news->

AT&T has experienced numerous breaches over the past years and while this latest breach may not have had a “material impact” on the company’s operations,⁶ it can and does have a material impact on its customers. This isn’t an issue exclusive to AT&T, as the 2023 T-Mobile data breach illustrates,⁷ or even to telecommunications companies, as a Kaiser Permanente data breach earlier this year demonstrates.⁸ Enshrining a data minimization rule in Federal law is a key to greater accountability for the many companies and industries that have persistently failed to adequately safeguard privacy and security.

We are repeatedly confronting—across industries and dozens of companies—the human costs of data breaches. A strong data minimization standard is an essential part of lowering the harms when data breaches inevitably occur. More broadly, a Federal privacy law that requires meaningful data minimization can help to ensure that companies’ data collection, use, and retention protects consumers and increases their trust in companies.

Question 2. How does data minimization support data security?

Answer. Data minimization requires companies to collect, use, share, and retain only what they need to provide a product or service. By narrowing the funnel of data held and handled at the collection stage, data minimization also reduces companies’ risk surface. A company cannot willfully misuse or accidentally mishandle data that it doesn’t have. And hackers cannot steal what isn’t there in the first place. In this most basic sense, data minimization is a key pillar of data security.

In addition, when a company is required to assess its own data collection and handling practices consistent with a minimization requirement, that company must critically assess its data governance decisions at every stage of the data life cycle (collection, use, and retention). These decisions include safeguarding against the potential misuse of data, weighing the risk of misuse against the current need for the data, and periodically assessing the utility of data holdings so that all data is not stored indefinitely by default. Responsible data minimization lowers the possible harms posed by breaches and other security incidents, and is thus a cornerstone of protecting consumers and companies, safeguarding privacy, and securing data.

In addition, organizations may have varying levels of technical capacity to implement data security measures and data audits. Although Federal privacy laws cover sectors like health, finance, and education, virtually every institution is likely to hold and use sensitive data—including data not covered by data security or privacy laws. A strictly sectoral approach to data security and privacy leaves unprotected many institutions and Americans who need a baseline level of support from a strong Federal standard for data minimization and other data security practices.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO
PREM TRIVEDI

Question 1. In the hearing, you stated that “GDPR gives too much deference to companies about what data minimization means” and that “there’s an opportunity for an American approach that’s different and works for us.” Can you elaborate on what specific data minimization requirements OTI would recommend within national privacy legislation?

Answer. A strong data Federal minimization standard in U.S. Federal law would have at least four core components: a strong substantive standard, clear permissible purposes for data processing, additional mechanisms for consumers to exercise control over their data, and a strong enforcement mechanism.

First, a Federal data minimization standard should operate as a substantive requirement, not merely a procedural one. A minimization standard that amounts to a check-box exercise in which companies disclose the purposes of data processing and then nominally comply with those purposes is not a meaningful minimization requirement. Instead, a specific substantive standard (like “necessary, proportionate, and limited to provide or maintain a product or service”) links minimization

events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

⁶AT&T Addresses Recent Data Set Released on the Dark Web, AT&T, Mar. 30, 2024, <https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html>.

⁷Nicholas Reimann, *T-Mobile Data Breach: Hackers Stole 37 Million Customers’ Info, Company Says*, Forbes, Jan. 19, 2023, <https://www.forbes.com/sites/nicholasreimann/2023/01/19/t-mobile-data-breach-hackers-stole-37-million-customers-info-company-says/>.

⁸Troy Wolverton, *Here’s what you should know about the Kaiser Permanente data leak*, San Francisco Examiner, May 7, 2024, https://www.sfoxaminer.com/news/technology/what-you-should-know-about-the-kaiser-permanente-data-leak/article_7d6f9256-0be7-11ef-a085-533bb1c22009.html.

to the “functionality of a product or service.”⁹ A substantive standard should be paired with authorization for the Federal Trade Commission to further define what constitutes compliance with the standard and to enforce it. Relatedly, a Federal data minimization standard should provide for heightened protections for processing sensitive data.

Second, a Federal data minimization requirement should clearly enumerate additional permissible purposes (like fraud prevention or protecting data security, to name two examples) for processing data. Identifying and appropriately scoping these permissible purposes provides meaningful flexibility for companies without creating exceptions—like a broadly construed permissible purpose to process data for product improvement—that could swallow up an entire minimization rule.

Third, a data minimization standard must be paired with a mechanism for consumers to take control over their data in ways that go beyond companies’ obligations to minimize data. This mechanism should include a universal opt-out mechanism that consumers can exercise with respect to further data collection and a data deletion tool for data already collected.

Fourth, a Federal data minimization rule must be paired with strong enforcement, which requires that the Federal Trade Commission be appropriately empowered and resourced to enforce the requirement. This multi-pronged approach to data minimization would avoid overly broad discretion to companies to decide what minimization means in practice, impose a strong substantive standard for minimization, and empower the Federal Trade Commission to further define that standard and enforce it.

Question 2. In your written testimony, you describe a “broken notice and consent approach in U.S. privacy law”. Should Congress require companies to clearly disclose their data privacy and security policies during the notice and consent process?

Answer. The Open Technology Institute (OTI)’s view is that a comprehensive privacy law should strengthen the substance of companies’ disclosures and make them more understandable to consumers. OTI therefore welcomes the approach in the American Privacy Rights Act (APRA) discussion draft that incorporates provisions of the TLDR Act.¹⁰

a. If you agree with the above statement that companies *should* clearly disclose their data privacy and security policies, please explain your perspective on the role that clear disclosure and informed consent play in protecting consumer privacy.

Answer. A strong data minimization regime is essential, but it does not remove the need for concise and meaningful disclosure. On the contrary, when paired with a legislative requirement to minimize data, meaningful notice and consent can help ensure responsible privacy and data governance. Consumers cannot make informed decisions without a clear understanding of companies’ data practices.

Our current U.S. data privacy regime of notice and consent rarely results in meaningful notice. Instead, people are usually granted a perfunctory moment of “choice” that most often leads them to accept terms they don’t understand or even read.¹¹ Addressing this issue by improving companies’ disclosures and data minimization practices can lead to stronger data protection and a renewed sense of agency and choice for people engaged in activities online.

b. Does OTI have any recommendations to ensure that disclosure and consent processes are clear and accessible?

Answer. Meaningful disclosure should be clear, truthful, and present critical information that consumers can actually use to make a decision about whether to proceed with using a product or service. Legislative requirements for company disclosures should be accompanied by strong, tiered enforcement while also allowing for appropriate flexibility via rules or guidance issued by the FTC. The TLDR Act is

⁹Jordan Francis, *Unpacking the shift toward substantive data minimization rules in proposed legislation*, International Association of Privacy Professionals, May 22, 2024, <https://iapp.org/news/a/unpacking-the-shift-towards-substantive-data-minimization-rules-in-proposed-legislation>. (“The majority of state comprehensive privacy laws . . . require controllers to limit the collection and processing of personal data to what is ‘adequate, relevant, and reasonably necessary’ to achieve the purposes that are disclosed to a data subject. Any unnecessary or incompatible secondary uses of personal data under these regimes require separate, affirmative consent. This rule can be labeled as ‘procedural data minimization,’ because whether or not collection or processing can occur turns on whether the controller has taken the correct procedural step—adequately disclosing processing purposes—rather than the substance of the processing activity.”)

¹⁰S. 2225, The TLDR Act, <https://www.congress.gov/bills/118th-congress/senate-bill/2225>.

¹¹See, e.g., Michelle Faverio, *Key findings about Americans and data privacy*, Pew Research, Oct. 18, 2023, <https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/>.

a recent example of proposed legislation that pairs meaningful disclosure requirements with appropriate regulatory rulemaking and enforcement.

The Act requires companies to provide a short-form summary of their terms of service on their websites, create graphic representations of data flows, and present their full terms of service in an interactive data format.¹² The short-form summary statement must include, among other things, the categories of sensitive information the company processes, directions for users to delete their information, and a list of data breaches over the last three years that the company was legally required to report.¹³ The Act requires the FTC to issue a rulemaking on the Act's core requirements and provides for enforcement by the FTC and state attorneys general (AGs).

Question 3. What role should the FCC have in protecting the privacy of consumers? Please explain OTI's recommendation for what the FCC's role should be within comprehensive privacy legislation.

Answer. The nation's communications networks are technologically complex and provide a uniquely comprehensive view into the lives and habits of their users. The FCC, as the government's expert agency on communications networks, already possesses the deep technical understanding necessary to protect consumer privacy in this sector. Congress recognized this in the 1996 Telecommunications Act when it gave the Commission specific and flexible authority under § 222 to protect consumer information. The FCC has exercised that authority by, for example, expanding the definition of protected consumer information in response to technological advances and requiring disclosure of data breaches of telecommunications providers.¹⁴ The FCC's core competence in protecting consumer privacy was on display in the April 29, 2024 fine of major wireless carriers and the focus on Internet service providers (ISPs) sharing customers' location data with data brokers.¹⁵

While it would be possible for another agency, such as the FTC, to replicate the FCC's existing expertise and capacity (if it were sufficiently resourced to do so), it would be the height of false economy to require that outcome in the name of "efficiency." It would be a mistake—and a decidedly inefficient allocation of government resources—to cast aside the FCC's existing expertise with respect to the privacy considerations specific to communications networks.

Instead, the FCC should be permitted to continue in its role as a complement to the FTC. This approach balances the FTC's broad purview and enforcement actions focused on business practices with the FCC's rulemaking ability and focused expertise on the privacy aspects specific to the operation of communications networks. And given the two agencies' long track record of working together, there's no need to force a false choice.¹⁶

Question 4. Does OTI believe that the American Privacy Rights Act bill draft sufficiently addresses data broker practices?

Answer. The American Privacy Rights Act (APRA) discussion draft (May 21, 2024) represents a useful first step toward holding data brokers accountable and empow-

¹² S. 2225, The TLDR Act § 2(a), <https://www.congress.gov/bill/118th-congress/senate-bill/2225>.

¹³ S. 2225, The TLDR Act § 2(c)(3), <https://www.congress.gov/bill/118th-congress/senate-bill/2225>.

¹⁴ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96–115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (2007 CPNI Order); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96–115, Declaratory Ruling, 28 FCC Rcd 9609, 9609–10, paras. 2–4 (2013) (2013 CPNI Declaratory Ruling).

¹⁵ *FCC Fines Largest Wireless Carriers for Sharing Location Data*, Federal Communications Commission, April 29, 2024, <https://www.fcc.gov/document/fcc-fines-largest-wireless-carriers-sharing-location-data>.

¹⁶ See, e.g., *FTC and FCC Sign Memorandum of Understanding on Continued Cooperation on Consumer Protection Issues*, April 30, 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-fcc-sign-memorandum-understanding-continued-cooperation-consumer-protection-issues>; *FTC Joins FCC in Renewing Memorandum of Understanding to Promote Cross-Border Law Enforcement Efforts to Combat Spam, Scams, and Illegal Telemarketing*, September 21, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-joins-fcc-renewing-memorandum-understanding-promote-cross-border-law-enforcement-efforts-combat>; *FTC and FCC Sign Memorandum of Understanding For Continued Cooperation on Consumer Protection Issues*, November 16, 2015, <https://www.ftc.gov/news-events/news/press-releases/2015/11/ftc-fcc-sign-memorandum-understanding-continued-cooperation-consumer-protection-issues>; *Joint FCC/FTC Policy Statement For the Advertising of Dial-Around And Other Long-Distance Services To Consumers*, March 1, 2000, <https://www.ftc.gov/legal-library/browse/joint-fcc-ftc-policy-statement-advertising-dial-around-other-long-distance-services-consumers>.

ering consumers. Notably, APRA § 112 requires data brokers to register with the FTC, allowing the agency to create a central registry through which consumers may submit a “Do Not Collect” request to all registered brokers. § 112 also supplements this prospective mechanism with a retrospective universal delete-my-data mechanism. APRA would thus allow consumers to meaningfully exercise their privacy rights with respect to data brokers, a sorely needed first step in addressing the power asymmetry between corporations and individuals. In addition, APRA would require data brokers to identify themselves as such on public websites that include a link to the FTC registry, prohibit them from engaging in certain actions, and direct the FTC to provide guidance on proper disclosure requirements for brokers.¹⁷

Other provisions of APRA may also have the effect of restricting the information that data brokers can now easily buy or collect online. For example, APRA prohibits companies from transferring sensitive information they collect to third parties without customers’ consent, provides opt-out rights for consumers, and requires companies to establish data security programs that minimize the harms of hacking.¹⁸ These provisions may reduce the information available to data brokers.

If passed, APRA would follow the enactment of U.S. legislation aimed at foreign governments’ ability to acquire information from data brokers. The Protecting Americans’ Data from Foreign Adversaries Act (PADFA), which passed in April 2024 as part of a supplemental appropriations bill, prohibits data brokers from selling Americans’ “personally identifiable sensitive data” to entities that are controlled by certain foreign adversary governments.¹⁹ While there appear to be loopholes through which data brokers’ sales to third parties could ultimately result in adversary governments acquiring data, PADFA’s objectives are laudable and may have some salutary effect by restricting data brokers’ direct sales to certain foreign governments.

But PADFA attempts to tackle only the downstream effects of one type of data brokers’ activities. APRA would directly empower consumers vis-à-vis data brokers. While APRA could go further in restricting the activities of data brokers, comprehensive privacy legislation requires bipartisan compromise. The draft bill makes important progress on regulating data brokers that sets the stage for future improvements.



¹⁷ American Privacy Rights Act of 2024 (discussion draft), May 21, 2024, https://d1dth6e84htgma.cloudfront.net/PRIVACY_04_xml_d1d6b82f10.pdf.

¹⁸ Derek B. Johnson, *Congressional privacy bill looks to rein in data brokers*, Cyberscoop, Apr. 15, 2024 <https://cyberscoop.com/congressional-privacy-bill-looks-to-rein-in-data-brokers/>.

¹⁹ PL 118–50, Division I: Protecting Americans’ Data from Foreign Adversaries Act of 2024, <https://www.congress.gov/bill/118th-congress/house-bill/815/text>.