

ENHANCING DATA SECURITY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

OCTOBER 6, 2021

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



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

U.S. GOVERNMENT PUBLISHING OFFICE

54-871 PDF

WASHINGTON : 2024

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota	ROGER WICKER, Mississippi, <i>Ranking</i>
RICHARD BLUMENTHAL, Connecticut	JOHN THUNE, South Dakota
BRIAN SCHATZ, Hawaii	ROY BLUNT, Missouri
EDWARD MARKEY, Massachusetts	TED CRUZ, Texas
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	MIKE LEE, Utah
BEN RAY LUJAN, New Mexico	RON JOHNSON, Wisconsin
JOHN HICKENLOOPER, Colorado	SHELLEY MOORE CAPITO, West Virginia
RAPHAEL WARNOCK, Georgia	RICK SCOTT, Florida
	CYNTHIA LUMMIS, Wyoming

MELISSA PORTER, *Deputy Staff Director*

GEORGE GREENWELL, *Policy Coordinator and Security Manager*

JOHN KEAST, *Republican Staff Director*

CRYSTAL TULLY, *Republican Deputy Staff Director*

STEVEN WALL, *General Counsel*

CONTENTS

Hearing held on October 6, 2021	Page 1
Statement of Senator Cantwell	1
Statement of Senator Wicker	3
Statement of Senator Baldwin	49
Statement of Senator Blunt	50
Statement of Senator Tester	52
Statement of Senator Fischer	54
Statement of Senator Klobuchar	55
Statement of Senator Cruz	57
Statement of Senator Hickenlooper	59
Statement of Senator Blackburn	61
Statement of Senator Blumenthal	62
Statement of Senator Moran	64
Statement of Senator Markey	66
Statement of Senator Scott	68
Statement of Senator Rosen	69
Statement of Senator Peters	72

WITNESSES

James E. Lee, Chief Operating Officer, Identity Theft Resource Center	5
Prepared statement	6
Jessica L. Rich, Of Counsel, Kelley Drye & Warren; Distinguished Fellow, Georgetown Institute for Technology Law and Policy	31
Prepared statement	32
Edward W. Felten, Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University; Former Chief Technologist, Federal Trade Commission	35
Prepared statement	36
Kate Tummarello, Executive Director, Engine	41
Prepared statement	43

APPENDIX

Response to written questions submitted to James E. Lee by:	
Hon. Amy Klobuchar	77
Hon. Kyrsten Sinema	77
Hon. Raphael Warnock	79
Hon. Roger Wicker	80
Hon. John Thune	84
Response to written questions submitted to Jessica L. Rich by:	
Hon. Amy Klobuchar	85
Hon. Roger Wicker	85
Hon. John Thune	86
Response to written questions submitted to Edward W. Felten by:	
Hon. Amy Klobuchar	86
Response to written questions submitted to Kate Tummarello by:	
Hon. Kyrsten Sinema	87
Hon. Raphael Warnock	88
Hon. Roger Wicker	95
Hon. John Thune	96

ENHANCING DATA SECURITY

WEDNESDAY, OCTOBER 6, 2021

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in room SR-253, Russell Senate Office Building, Hon. Maria Cantwell, Chair of the Committee, presiding.

Present: Senators Cantwell [presiding], Klobuchar, Blumenthal, Markey, Peters, Baldwin, Tester, Rosen, Hickenlooper, Warnock, Wicker, Thune, Blunt, Cruz, Fischer, Moran, Blackburn, Young, and Johnson.

OPENING STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

The CHAIR. The Committee on Commerce, Science, and Transportation will come to order. Today, we are having a hearing on enhancing data security. And this is the second in a series of hearings that we are having on the importance of good Federal standards for both privacy and data security.

Our first hearing focused on the empowerment of the FTC with new resources and the Data Privacy Bureau that is being considered as part of our reconciliation negotiations, as well as hearing from the witnesses what we should be doing to enhance further data privacy. Today, we want to focus on data security and the fact that we are seeing record levels of breaching and intrusions on the privacy of American individuals.

Our hearing today, we will hear from a great list of witnesses that I will mention and will formally introduce in a few minutes. The data systems that we rely on today are very vulnerable. We are experiencing increasing rates of data breaches and now seeing sophisticated actors impacting hundreds of millions of American consumers. I think that we are going to hear from Mr. Lee's report that 2021 will again set a record year for the number of data breaches and concerns to consumers in the United States. What is troubling about that is that every year we are breaking records.

What is troubling is that these breaches are now more sophisticated and that we don't have the adequate security to help stop them. Earlier this year, a hacker took Colonial Pipeline offline, causing fuel shortages across the East Coast. Ransomware attacks on hospitals have put patients' lives at risk. We heard yesterday about Facebook going offline globally due to faulty configuration, and there is word out this morning that Amazon may be facing its own situation today. So part of the problem is that we live in a

more connected world, and what we know now is that when there is a data breach, that consumers are the ones that pay the heavy price.

We do not have enough on the books and a Federal standard to make sure that companies are more accountable to these breaches. Senator Wicker and I both introduced legislation trying to set a Federal data security standard in the United States. We agree that we need to monitor these systems for threats and vulnerabilities, patch their system softwares when they needed updates, make individuals who serve as data privacy officers to be more efficient in their oversight, and we agree that the Federal Trade Commission should enforce these standards along with Attorney Generals.

We believe that these companies don't invest enough for the fact that they have oversight to our precious data and information, so we need to act. Massive amounts of personal data are collected from Americans every day as they go online to connect with family, pay bills, work, obtain medical information, send their kids to school. And yesterday was an example of the data that was being collected on children and the offense that we all took to that information and data. Data is collected on Americans, whether they like it or not. And we all know stories of data brokers and the breaches behind the scenes where data was collected without anybody's actual acquiescence to that.

So today, Mr. Lee, who is with the Identity Theft Research Center, a nonprofit organization dedicated to helping identity theft victims, will be testifying. And according to the ITRC's third quarter 2021 breach analysis report, we will again see a record year of breaches in the United States and that these tactics are putting people in greater risk. That is very concerning to me in the State of Washington, where in 2020 we saw seven times the rate of identity theft complaints to the FTC over 2019.

So this means that 2021 is going to continue to have an even larger number. Hackers are specifically targeting data like login, the passwords, and often re-use them across multiple accounts, unlock access to accounts, and cybercrime is lucrative, and the data breaches that we are seeing, not only as I said compromise our data, but are now a big business of cyber and ransomware attacks. The number of reported data breaches in the first 9 months of 2021 exceeded last year's 12 month by 17 percent. So the numbers keep rising and we are on to another record breaking year.

About 160 million individuals had their data compromised from July of this year to September 21. There have been more ransomware attacks in the first 9 months of 2021 than in both 2019 and 2020. And the number of cyber-attacks so far this year has already surpassed the total number of all data compromises in the year of 2020. So these intrusions take a real toll on people. Last year, the State of Washington was swept with an insurance fraud as it related to unemployment benefits.

Later in the year, the Washington State Auditor's Office, which had been receiving unemployment fraud claim, had its data compromised due to that vulnerability in the legacy system that was provided by a third party, Accellion. Accellion's systems were breached throughout the country, and we still don't know the extent of that breach. But in Washington, the personal information

of 1.6 million residents was stolen. So we know that the identity theft can have a devastating impact on individuals who can't obtain unemployment benefits because a criminal has already applied for them. 40 percent of these victims were not able to pay their bills. 14 were evicted for not paying rent. 33 percent did not have enough money for food and utilities. 13 percent were not able to get a job.

So while most identity theft victims lose less than \$500, 21 percent of these victims report losing more than \$20,000. And these are a lot of people growing every year in numbers. So we need to act to inform better national standard for data security, to protect Americans' personal data and privacy so they are less at risk. That is why we introduced the Consumer Online Privacy Act, COPA, last Congress, along with my colleagues here on the Committee, Senators Schatz, Klobuchar, and Markey, and to continue to grow and strengthen our Federal statutes so we can address these issues.

So we look forward to hearing from the witnesses today about those particulars on how we strengthen these standards, what we need to do to protect whistleblowers, what we need to do to report data security and privacy problems, and what we can do to better protect the public. We know that a stronger FTC will help, but we need to give the FTC the resources that they need to do their job. So I again will introduce the witnesses in a few moments, but I think we have a very distinguished panel here to hear from on these important issues.

So now I will turn to the Ranking Member for his opening statement.

**STATEMENT OF HON. ROGER WICKER,
U.S. SENATOR FROM MISSISSIPPI**

Senator WICKER. Thank you, Senator Cantwell. Appreciate it very much. Good morning to our witnesses. Each year, Americans benefit from a growing supply of digital products that make life better. At the same time, they also collect, share, and sell our personal data.

Although this data could provide meaningful insights about consumer preferences, it has become a target for bad actors seeking to exploit people's data for nefarious purposes. According to reports, data breaches have gone up by 38 percent this year alone. These include phishing attacks, ransomware attacks, supply chain attacks and more. The average cost of a data breach in the United States is roughly \$8 million. But the cost for the broader public is hard to measure. Data breaches can bring long-term damage to reputations, personal finances, and even to physical safety.

When Congress passed the FTC Act in 1914, the Federal Trade Commission was given the task of protecting consumers from deceptive and unfair commercial practices. The Commission has rightly used this authority to curb business practices that put consumers' personal information at risk. This required companies to adopt stronger protections for consumer data and in some instances implement safeguards such as employee training, maintaining access controls, and monitoring systems for data security incidents. The FTC also continues to inform the private sector on best practices to prevent security breaches. Importantly, the FTC's long

standing approach to data security has been based on reasonableness. With cyber threats constantly evolving and growing more complex, there is no single or perfect solution to the problem.

The FTC needs the flexibility to adjust to constantly shifting cyber threats. Under the Obama Administration, the Commission asserted this standard of reasonableness in a bipartisan statement. I am going to quote what the Commission said, “a company’s data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. There is no one-size-fits-all data security program. The mere fact that a breach occurred does not mean that a company violated the law.”

Although this remains true today, there is certainly more that Congress can and should do to make consumer data safer and protect Americans from cybercrime. In July, Senator Blackburn and I introduced the Safe Data Act, which would give the FTC more tools and authorities to improve data security practices in the marketplace and deter cyber criminals. Our legislation would require covered entities to minimize the amount of personal consumer data they collect and retain. Would require businesses to maintain certain internal controls to reduce risks to data. It would give the FTC targeted rulemaking authority to ensure companies can identify security vulnerabilities. It would expand the FTC’s jurisdiction over common carriers and nonprofits and to make sure companies follow the law. Our bill would allow the FTC to impose civil penalties for first time offenses. Many of these ideas represent areas of bipartisan common ground among members of this committee.

Today’s hearing is an opportunity to discuss these and other steps and improve data security through bipartisan Federal privacy legislation. As I said last week, Americans deserve to have their data protected. Now is the time for Congress to act to pass legislation that protects the American people’s privacy and personal information. Thank you, Senator Cantwell.

The CHAIR. Thank you, Senator Wicker. And again, welcome to the witnesses. We are joined by Mr. James Lee, who is Chief Operating Officer of Identity Theft Resource Center, a nonprofit organization dedicated to helping identify identity theft victims and analysis reports that are so helpful. In fact, I think we have—part of your record is a pretty healthy report on this year’s data. We would also like to welcome Ms. Jessica Rich, who is currently counsel at Kelly Drye, former Bureau of Consumer Protection at the Federal Trade Commission, where you had experiencing a vast number of roles of the FTC, including the agency’s Bureau of Consumer Protection Director, where you oversaw actions against companies who failed to uphold their promise to consumers.

So, thank you for being here. In addition, we have Ed Felten, who is the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton and former Chief Technology—Technologist, I think that was the title at the Federal Trade Commission. So we look forward to hearing your comments as it relates to your time there and now and understanding the marketplace.

And finally, Ms. Kate Tummarello, is that right? Tummarello, who is Executive Director of Engine, a nonprofit startup advocacy

group, to discuss the importance of data security and the ecosystem. So, welcome to all of you. Thank you for being here. We will start with you, Mr. Lee.

**STATEMENT OF JAMES E. LEE, CHIEF OPERATING OFFICER,
IDENTITY THEFT RESOURCE CENTER**

Mr. LEE. Good morning, Chair Cantwell, Ranking Member Wicker, the rest of the Committee. Thank you for the honor of speaking with you today. My name is James Lee. I am the Chief Operating Officer of the nonprofit Identity Theft Resource Center. We are based in San Diego, California. The chair was very kind to share a lot of our data for this morning that we just released in our Q3 data breach report. So I am not going to talk about those numbers as much as I am now going to talk about the impacts, but I will say that we are now, as of today, only 238 data breaches away from an all-time high. And we had 446 data breaches in this quarter.

So, you do the basic math. We are in for raising the bar substantially. Let's discuss the real world example of what I am talking about, which is poor cybersecurity leads to data breaches which leads to identity crimes. That is the value chain we are talking about. And let us talk specifically about the identity related unemployment fraud. The ITRC advisors first realized there was a problem last year when we started getting calls from Seattle. Now we don't get a lot of calls about unemployment fraud. Shortly after the Federal unemployment subsidies went into effect, we started to receive one call a day. That then became a couple of calls a day.

And very quickly it became where we had more contacts in 1 month than we had seen from all 50 states in 2 years. It was a rapidly increasing problem. In 2019, we logged 14 cases of identity related unemployment fraud, from March 2020 through last week. The ITRC has logged 2,112 cases of unemployment identity fraud in all 50 states and the District of Columbia, and it continues today. Behind all those numbers, though, are people, they are victims. And the victims in this case fall into two cases, people who are still employed, but whose information was misused to apply for benefits they did not need. They were largely inconvenienced. But they are still at risk, increased risk of future crimes because their data is in the hands of criminals.

But for the victims who are denied benefits, these cyber criminals got the money first. And our research shows, as the Chair noted, 40 percent were unable to pay their bills, 14 percent were evicted, 33 percent could not pay for food. As of April this year, we found that 69 percent of the victims denied benefits last year still had not resolved the issues as of this year. All of these issues are directly linked to identity criminals misusing stolen personal information, largely from data breaches, often directly linked to poor cybersecurity practices, procedures, and execution.

Which begs a very simple question with a very complex answer, what do we do? In the ITRC's view, the status quo is broken. We believe policymakers and industry leaders need to work together to focus on three key areas, which I am now going to talk about. We need better cybersecurity standards and practices. For example, cyber-attacks against known but unpatched software flaws that come from data breaches, they lead to data breaches, result—those

results are largely preventable. You can prevent those kinds of cyber-attacks. Another highly effective tool, don't collect the information if you don't need it. And if you are through with it, get rid of it. You cannot breach what you do not have. A very simple concept.

But without enforceable minimum standards, there are no broad incentives beyond trying to avoid headlines or post breach litigation that get people to actually make the broad organizational changes that are often needed. We need better enforcement. We believe victims are best served when there are options for redress. In today's environment, where some states are more aggressive in protecting their citizens than others, the result is often disparate victim support for the same crime, but what you are able to get accomplished for the victim varies by where you actually are.

Technology moves faster than Government, so state and local jurisdictions need the ability to be responsive to new threats and technologies while maintaining a minimum base of strong security and privacy. And we believe our partners at the FTC are best equipped to be that enforcement agency. Finally, our victim notification system is wholly inadequate. The first U.S. data breach law was proposed in 2003 by a certain Senator from Washington. California lawmakers took that and actually passed a data breach law that same year. Since then, the average number of data breaches reported in the United States has grown to about five a day.

The average number of data breaches reported in the European Union is 331 a day. Couple that with the estimated 15 billion stolen logins and passwords available for sale in the digital marketplaces at any given time, and it is pretty obvious that data breaches are underreported in the United States. In our view, today's hearing is ultimately about how we reduce the number of identity crime victims. Yet, there is a separate conversation we also need to have about how we support people when they are victimized.

That victim support system we have today is just as inadequate as our cyber security standards, our enforcement structure, and our system of victim notification. The ITRC would love to talk to you about that too sometime. Thank you for your time and attention, and I look forward to answering any questions you may have.

[The prepared statement of Mr. Lee follows:]

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

Introduction

Good morning, Chair Cantwell, Ranking Member Wicker and members of the Committee. 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 the past 21 years, the ITRC has offered free assistance to victims of identity crimes. Through our contact center staffed by trauma-informed advisors, about 11,000 times per year we directly help victims recover their identities that have been stolen or otherwise compromised and we help consumers who want to prepare for the day when their personal information is acquired or misused by identity criminals.

Through our website and outreach programs, we help educate an additional one million people around the world who hold U.S. identity credentials, including military personnel, on how to protect their identity information. We also provide infor-

mation about the latest scams that involve the theft or misuse of personal information.

Since 2005 the ITRC has compiled the largest repository of publicly noticed data breaches and other forms of identity data compromises. What started as a handful of data points 16 years ago with a single company notice has grown into a database of more than 13,000 data breaches with as many as 90 data points per event that is updated daily.

We also publish an *annual data breach report* and quarterly updates that analyzes the trends reflected in the data breach notices mandated by state law and Federal regulations. In fact, earlier today, we published our *Q3 Data Breach Analysis* which shows we have already surpassed the total number of U.S. data compromises reported in full-year 2020. We are only 238 data compromises from tying the all-time record set in 2017. You'll find the full report as an attachment to my written testimony. **Exhibit A: Q3 2021 ITRC Data Breach Analysis—October 6, 2021**

I would like to briefly mention two additional reports that we publish. First, our Consumer Aftermath Report is the only comprehensive study on the total impact of identity crimes on consumers. I will reference our most recent findings report later in my remarks and the full report is attached as an exhibit. **Exhibit B: 2021 Consumer Aftermath Report, May 2021**

Later this month, which coincidentally is Cybersecurity Awareness Month, we will publish our first report on the impacts of security and data breaches on small businesses and solopreneurs including gig workers. Our *Business Aftermath Report* is the first independent research of its kind that is based on information taken directly from small business owners and leaders.

Finally, as a non-profit, the ITRC is funded primarily through grants from the Department of Justice, Office of Victims of Crime as well as private contributions and corporate sponsorships. We work closely with key Federal agencies on issues that involve identity crime victims including the Federal Trade Commission (FTC), the Internal Revenue Service's Security Summit, the Pandemic Response Accountability Committee (PRAC), the Department of Homeland Security (DHS), and numerous state and local law enforcement agencies. For example, the FTC has referred more than 20,000 victims of the most complex identity theft cases to us to provide the specialized support many ID crime victims require that government agencies and large for-profit companies are not equipped to address.

The connection between cybersecurity, data breaches, and identity crimes

Our job, every day, is to talk with victims of identity crimes. The information I'm going to share with you today is largely based on what we learn from people directly impacted by these crimes. These interactions also influence our advice to the Committee today.

When the ITRC was born two decades ago, the primary source of identity crimes was physical—stolen mail, a lost laptop, dumpster diving, shoulder surfing, a file folder left on a desk, or a filing cabinet left unlocked. The criminal was likely someone you knew or shared a connection.

Even when California passed the first data breach notice law, the first nationwide data breach notice didn't involve a cyberattack—it was the result of organized criminals setting up a legitimate-looking insurance business for the purpose of ordering paper copies of credit reports from a data broker. My how things have changed.

Today, the primary source of data compromises involving personal information is related to cyberattacks launched by professional criminals outside the U.S. or by Nation/States. Of the 1,291 publicly reported data compromises so far in 2021, 1,111 are the result of a cyberattack. The number of ransomware-related data compromises reported so far in 2021 *exceed* the number of similar events in 2020 & 2019 *combined*. It should be noted that the 1,111 cyberattack-related data events reported so far this year is more than *all data compromises in full-year 2020*.

The chart below from the *Q3 Data Breach Analysis* shows the various ways data compromises occur and the most common attack vectors used by cybercriminals. Far and away phishing and related attacks followed by ransomware are the most common forms of cyberattacks that lead to data compromises.

Attack Vector 2021 YTD vs. Full Years 2020 & 2019			
Attack Vector	2021 YTD	2020	2019
Cyberattacks	1,111	878	928
Phishing/smishing/BEC	370	383	490
Ransomware	244	158	83
Malware	103	104	112
Non-secured Cloud Environment	19	50	15
Credential Stuffing	12	17	3
Unpatched software flaw	2	3	3
Zero Day Attack	2	1	n/a
Other - not specified	359	162	222
System & Human Errors	134	152	231
Failure to configure cloud security	48	57	56
Correspondence (email/letter)	40	55	89
Misconfigured firewall	9	4	4
Lost device or document	7	5	19
Other - not specified	30	31	63
Physical Attacks	35	78	118
Document Theft	3	15	19
Device Theft	12	30	57
Improper Disposal	3	11	14
Skimming Device	n/a	5	4
Other - not specified	17	17	24
Unknown	11	n/a	2
TOTALS:	1,291	1,108	1,279

What has also changed over time is the type of data identity thieves want and how they acquire it. The last time we set an all-time high for data breaches in 2017, identity thieves wanted to Hoover up as much data as possible from as many sources as they could find.

Today, we see highly organized cybercriminals launching highly sophisticated attacks using automated tools. Data quantity is no longer the goal of an attack; data quality is. With the right information—primarily logins and passwords—cyberthieves do not need to engage in time consuming and risky attacks that exploit known, but unpatched software bugs. Using automated tools and data stolen in breaches, they can walk in the front door and have access to everything they need to extort an organization or take over the account of an individual.

As a result of this shift, we see more cyberattacks that impact fewer individuals in mass attacks. Make no mistake, though, individuals are still at-risk today.

We are moving from an era of identity theft where data is acquired and accumulated to a time of identity fraud where ID thieves monetize the data they've collected—with the occasional effort to refresh older information. The chart below shows the shift in terms of the number of data breach victims dating back to 2015.

Compromise Year-over-Year Totals		
Month	Compromises	Victims
2021 YTD*	1,291	281,451,400
2020	1,108	310,116,907
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,529	1,827,986,798
2016	1,105	2,541,588,745
2015	785	318,276,407
* As of 9/30/2021		

Connecting the Dots

To connect the dots using a real-world example, let's discuss the dramatic rise in identity-related unemployment benefits fraud during the COVID-19 pandemic. Public and private sector estimates of the financial impacts vary from just short of \$100B to nearly \$400B in stolen benefits. The victims fall into two categories: those who needed benefits and were denied because a cybercriminal applied for the benefits first; and those who didn't lose their job, but someone applied for and received benefits in their name.

At the ITRC, we first noticed there was something unusual occurring when we began to receive phone calls from Washington State. In normal times, the ITRC receives fewer than 20 inquiries per year about identity-related unemployment fraud. Shortly after the Federal unemployment subsidies went into effect, we began to see a call a day from the Seattle area. That soon increased to several a day, before leaping to more contacts in one month than we had seen from all 50 states in the previous two years. **Exhibit C: Spreadsheet of 2020-21 ITRC Victim Stats by State**

In early 2020 Washington State had a robust unemployment benefits program and had recently upgraded its technology to a state-of-the-art system that allowed taxpayers to register for a single account to access all State services. The system included a credential verification process that relied on readily available information about a person—information that was available for sale in identity marketplaces along with known logins and passwords. It was very easy for cybercriminals to use stolen information to create a new State benefits account or redirect an existing account using data breach-fueled information.

The volume of applications overwhelmed the state teams responsible for auditing the applications for fraud, eventually leading to the decision to switch from identity verification before paying benefits to auditing for fraud after-the-fact. After one month, Washington state change their model and reports of fraudulent unemployment claims dropped dramatically, but not before more than \$500M in fraud was identified in Washington State alone.

Since April 2020 through today, 98 Washington residents have sought the assistance of the ITRC to help them recover from government benefit related fraud. I've attached to these remarks a state-by-state breakout of residents who turned to the ITRC for assistance since 2019.

Soon, this scenario played-out in every state to one degree or another. Ironically, the states with technology dating back to the 1960s fared the best. And at least one state that upgraded mid-pandemic saw their cyber-related fraud increase AFTER they implemented a state-of-the-art system. From March 2020 to the end of September 2021, we logged 2,112 cases of unemployment identity fraud in all 50 states and the District of Columbia.

Behind all these numbers, though, are victims. Real people who were—and in some cases still are—suffering.

The ITRC's *Consumer Aftermath Report* from May of this year illustrates the impacts of this fraud on two distinct groups. However, as you will see, the impacts are not proportionate.

Victims whose identities were used to apply for benefits they didn't need were largely only inconvenienced. They are still at risk of future attacks, however, be-

cause their information has been compromised and is in the hands of known criminals who can use that information at any time.

Of course, they may not have known their identities were being misused until a debit card arrived in the mail loaded with unemployment benefits. Often-times the letter was followed by a call from someone claiming to be a representative of the State or issuing bank saying there had been a mistake and to send the card to a “special” address.

Or a victim or mail carrier would find someone trying to collect mail from their mailbox. In some incidents reported to the ITRC, as many as 50 debit cards per day would arrive by mail—each addressed to a different person. Others didn’t learn their identities had been compromised until they received a 1099 form saying they owed taxes on benefits they did request or receive.

For the victims who needed those benefits but were denied the resources they were due, the impacts could be devastating. In following up directly with victims, we learned that:

- 40 percent were unable to pay their routine bills
- 14 percent were evicted for non-payment of rent or mortgage
- 33 percent did not have enough money to buy food or pay for utilities
- 13 percent were unable to get a temp or permanent job as a result of identity misuse

As of April 2021 when this survey of victims was conducted:

- 69 percent of victims denied benefits said their issues were still unresolved from 2020
- 75 percent of victims whose identities were used to apply for PPP loans had unresolved issues
- 82 percent of people who were the victims of benefits scams where they unknowingly paid a criminal to expedite their benefit payments had not resolved the issues from 2020.

And, the fraud continues to this day. A local television station here in Washington, DC reports that one local *Virginia business continues to receive requests to verify unemployment claims*—none of which are for actual employees of the company. In 2020 we opened 802 unemployment ID fraud cases. To date in 2021, the count stands at 1,296. In 2019, the count was 14.

All of these issues are directly linked to identity thieves stealing personal information. While it’s not possible to always draw a direct line to a specific data breach, the broad-based attacks that impacted every state utilized data available in illicit identity marketplaces. Information placed there as a result of an organizational failure to prevent unauthorized access to consumer information, most often because of poor cybersecurity practices, procedures, or execution.

All of this begs a simple question with a complex answer: What can, and should, we do?

In the ITRC’s view, all potential solutions begin from the same place: The status quo is broken. From there, we believe policymakers and industry leaders need to focus on three key areas to achieve the ultimate goal of any public policy: Protect our citizens and protect the homeland. Specifically, we recommend intense focus on three areas:

We need better cybersecurity standards and practices.

The cyberattacks against known, but unpatched flaws and the data breaches that result from them are largely preventable.

NIST has set a record each year since 2016 for the number of known software flaws that are assigned a risk rating in the *National Vulnerability Database*. We will set another record this year, too, most likely in excess of 19,000 known software bugs. There have already been 33 Zero Day attacks—cyberattacks exploiting a previously unknown software flaw—in calendar year 2021. That’s 11 more than 2020.

Meanwhile, the average *time to patch a known software bug* in enterprise software or web applications is measured in months or years depending on the sector—while attackers can exploit a new flaw in a matter of hours or minutes. Without enforceable minimum standards, there is no incentive beyond headline avoidance and fear of post-breach litigation to motivate most organizations. The “it’s cheaper to pay the fine” mentality is alive and well when it comes to cybersecurity.

There is an even more basic step that can be highly effective at keeping personal information out of the hands of criminals: don’t collect the information in the first place. You cannot breach what you do not have. Americans have made it pretty clear when given a choice about opting in or out of data collection or sharing, most

people will say “no thanks.” An estimated *six percent (6 percent)* of U.S. iPhone users opted-in to data tracking when given the opportunity to choose earlier this year. That’s six percent of an *estimated 116M* people in the U.S.

We need better enforcement.

Victims deserve better enforcement mechanisms and we believe victims are best served when there are options for redress. Clearly, the sticking points here in Washington and the states that have considered their own privacy & security laws are the issues of private right of action and Federal pre-emption. When regulators have the tools they need to fully enforce strong laws, everyone wins. However, in the environment where we operate today, some states are more aggressive in protecting their citizens than others, resulting in disparate impacts for the same crime based on where you live. Victims and businesses alike are well served when everyone knows the rules and faces the same consequences. And just like in other areas of public policy, a system where the government and the aggrieved share the ability to seek redress provides the options that helps everyone.

The current California privacy law—the CCPA—is an example of that shared authority. Only the *California Attorney General* may take an enforcement action under most provisions of the law—the exception being if a data breach is caused by a failure to provide adequate cyber security. Then the law sets a procedure by which an individual can seek a statutorily set level of damages. This limited right of action is included in the new privacy law overwhelming approved by voters in 2020 that will take effect in 2023. The new CPRA also allows a slightly expanded private right of action if an e-mail address and password are compromised in a data breach.

As for Federal pre-emption, again we believe victims are best served by options. While we need minimum standards, technology moves faster than government. Giving state and local jurisdictions the ability to be responsive to new threats and technologies while maintaining a base of strong security and privacy is the kind of flexibility we believe helps victims and organizations, too.

Lastly on this point, our partners at the FTC are best equipped to be the enforcement agency for enhanced privacy and protection standards—if they are given the proper tools, mechanisms, and Congressional mandate.

Our victim notification system is wholly inadequate.

Please understand that what I’m about to say is not a rousing endorsement of the European Union’s General Data Protection Regulation (GDPR). But, one area where the GDPR seems to be working is the breach notification system wherein organizations are required to provide notice to regulators and, ultimately, citizens if appropriate.

Why do I say this is a model worthy of exploration? The concept of a U.S. data breach notice law was first proposed in 2003 by a certain senator from Washington. Congress did not adopt the law, but California lawmakers took notice and passed the world’s first data breach notice law that same year. It became effective in 2004. In 2005, “data breach” entered the popular lexicon for the first time when a company where I was an executive issued the first nationwide breach notice under the theory that data doesn’t respect dotted lines on a map. . .and with a little friendly persuasion from Sens. Markey and Blumenthal in their previous roles.

By the way, that breach was quaint by today’s standards—156,000 potential victims, as Ms. Rich may remember—and would not even meet the threshold for issuing a data breach in some states today. Over the next 13 years, 90 other countries adopted data breach laws before the final two states required breach notifications in the wake of the Equifax compromise in late 2017.

I already mentioned that the ITRC database reflects some 13,000+ data breach notices accumulated over 16 years. The current average number of breaches reported in the U.S. is about 5 per day. The *average number of data breaches* reported in the EU under the GDPR is 331 per day as of January 2021. Couple that with the estimated 15B stolen logins and passwords available for sale in identity marketplaces and it’s obvious the number of U.S. data breaches are being under reported.

When they are reported, the notices are largely meaningless with little transparency or actionable information. A recent study by the *University of Michigan* and a second by *Carnegie Mellon University* both show that we simply are not equipping victims with enough information about what happened and how to protect themselves. The vast majority of breach victims simply do nothing.

The Michigan study concluded that even after receiving a breach notice, most people in the study did not know their information had been compromised at least three times. The Carnegie Mellon study showed that most people who receive a data breach notice do not take even the basic step of changing the password on a com-

promised account; and if they do, it's generally months after receiving the breach notice and the replacement password is weaker than the original.

Mandatory reporting with strong penalties for failing to comply with both the required form and substance of a notice along with a bias toward more transparency will make a difference in terms of equipping victims with the knowledge needed to protect themselves and their loved ones from future data compromises.

Conclusion

In our view, today's hearing is ultimately about how we reduce the number of identity crime victims. Yet, there is a separate conversation needed about how we support people when they are victimized. The victim support system we have today is just as inadequate as our cybersecurity standards, our enforcement structure, and our system of victim notification. The ITRC would love to engage with you on this topic, too.

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



Exhibit A



Third Quarter 2021 Data Breach Analysis: Number of 2021 Data Compromises Surpasses Total Number of Compromises In 2020

Key Takeaways

- The number of publicly-reported data compromises through September 30, 2021 has exceeded the total number of events in FY 2020 by 17 percent, even though the number of compromises dropped by nine (9) percent compared to Q2 2021. The trendline continues to point to a record-breaking year for data compromises.
- The number of data compromise victims dramatically increased in Q3 - ~160M individuals primarily due to a series of data exposures¹ in the Quarter.
- The total number of cyberattack-related data compromises YTD is up 27 percent compared to FY 2020, with Phishing and Ransomware far and away the primary attack vectors.
- There have been no publicly reported data compromises to date in 2021 attributed to payment card skimming devices.
- There is a disturbing trend developing where organizations and state agencies do not include specifics about data compromises or report them on a timely basis. One state has not posted a data breach notice since September 2020.

Discussion

- The total number of publicly reported data compromises dropped slightly in the Third Quarter (Q3) ending September 30, 2021 (446 in Q3 vs. 491 in Q2). However, the total number of data compromises for the year to date (YTD) has surpassed the total of publicly-reported data events in 2020: 1,291 compared to 1,108, a 17 percent increase. The current trendline indicates the total number of data compromises in 2021 will exceed the previous all-time high set in 2017 of 1,529². The current delta is 238.
- Meanwhile, the number of individuals impacted by a data compromise in Q3 surpassed the total number of victims reported in the first six months of 2021 - ~160M victims in Q3 compared to ~121M in Q1 and Q2 2021 combined. The dramatic rise in the number of victims was directly related to 26 instances where cloud databases were not secured. Six (6) cyberattacks against unsecured databases impacted ~48M victims. Twenty (20) organizations failed to secure a cloud database exposing the personal information of 99M individuals. Data exposures due to a system or human error are generally lower risk because there is no indication the information was accessed, copied, or removed from the exposed database.
- Adjusting for the large increase in victims of data exposures and unsecured cloud database attacks, ~13M individuals were impacted by all other forms of data compromises. That corresponds to the continuing macro trend of fewer individuals being impacted by mass data breaches related to cyberattacks.





- Cyberattacks remained the primary cause of data compromises, including data breaches, data exposures, and data leaks. Phishing and related attacks in 2021 (370 to date) will likely exceed the 383 similar attacks reported in 2020. The 244 ransomware-related data compromises reported to date in 2021 exceed the 241 similar events in 2020 & 2019 combined.
- There have been zero (0) data compromises attributed to skimming devices so far in 2021. Skimmer-related data breaches have been steadily declining since 2015 with the introduction of chipped payment cards as required by PCI security standards.
- Data compromises were up in 10 out of 13 sectors in Q3 2021 compared to Q3 2020, and nine (9) out of 13 sectors saw more compromises compared to Full-Year (FY) 2020. Financial Services, Manufacturing & Utilities, and Education have seen the largest increases; Healthcare and Professional Services have seen slight decreases.
- Supply Chain attacks continue to have a meaningful impact on both companies and individuals. Although Supply Chain attacks only count as a single attack, they impact multiple organizations and the individuals whose data is stored by them. Sixty (60) entities were impacted by 23 third-party/supply chain attacks, including eight (8) attacks that were reported in previous Quarters. Nearly 793K individuals were impacted in Q3.
- There has been an increase in a lack of transparency in breach notices at both the organization and government level that, if it continues, could lead to a significant impact on individuals. See the categories in the charts below that indicate the growth in the number of events with little or no detail (Other). Academic research^{3,4} shows that the majority of individuals already fail to acknowledge or act on data breach notices. Withholding important information or failing to post notices on a timely basis may serve to prevent individuals from taking actions to protect their identities. For example, one state has not posted a new data breach notice on its website since September 2020.

Q3 2021 Data Compromise Details

Number of Compromises Q3

- **Data Breaches:** 417 data breaches; 61,003,474 victims
- **Data Exposures:** 20 data exposures; 99,128,886 victims; 189,552,977 total records exposed
- **Data Leaks:** One (1) data leak(s); 700,000,000 victims (includes non-U.S. victims)
- **Unknown Attack Vector:** Eight (8) unknowns; 3,172 victims





Attack Vectors Q3 2021

- **Cyberattacks:** 389 breaches/exposures; 60,866,744 victims
 - 124 Phishing/Smishing/BEC
 - 91 Ransomware
 - 33 Malware
 - Six (6) Non-secured cloud environment
 - Four (4) Credential Stuffing
 - Two (2) unpatched software flaw
 - One (1) Zero Day Attack
 - 128 Other – not specified
- **System & Human Errors:** 43 breaches/exposures; 99,256,777 victims
 - 20 Failure to configure cloud security
 - 10 Correspondence (email/letter)
 - Four (4) Misconfigured firewalls
 - Two (2) Lost device or document
 - Seven (7) Other – not specified
- **Physical Attacks:** Six (6) breaches/exposures; 9,882 victims
 - Two (2) Document Theft
 - One (1) Device Theft
 - Three (3) Other – not specified
- **Supply Chain Attacks:** *(included in the attack vectors above)*
 - 60 entities were impacted by 23 third-party/supply chain attacks, including eight (8) attacks that were reported in previous Quarters; 793,052 victims in Q3
 - 57 entities affected; 673,447 victims from third-party/supply chain cyberattacks
 - Two (2) entities affected; 2,707 victims from third-party/supply chain systems and human errors
 - One (1) entity affected; 116,898 victims from third-party/supply chain physical attacks
 - Noteworthy Supply Chain Attacks
 - **Blackbaud (2020):** The ITRC has recorded 580 entities with 12,813,995 victims from the Blackbaud data breach. One-hundred (100) (of the 580) entities with 252,923 victims reported in 2021.
 - **CaptureRX:** The ITRC has recorded 162 entities impacted
 - **Accellion:** The ITRC has recorded 38 entities impacted
 - **Netgain Technologies, LLC (2020):** The ITRC has recorded 23 entities impacted
 - **ParkMobile:** The ITRC has recorded 19 entities impacted
 - **Herff Jones:** The ITRC has recorded 12 entities impacted
 - **Med-Data:** The ITRC has recorded six (6) entities impacted





Charts

Compromise Year-over-Year Totals		
Month	Compromises	Victims
2021 YTD*	1,291	281,451,400
2020	1,108	310,116,907
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,529	1,827,986,798
2016	1,105	2,541,588,745
2015	785	318,276,407

*As of 9/30/2021

Compromises YTD 2021 by Month		
Month	Compromises	Victims
JAN	100	7,385,411
FEB	111	35,320,708
MAR	144	23,309,513
APR	151	25,667,485
MAY	137	21,393,693
JUN	203	8,239,058
JUL	163	7,363,216
AUG	158	151,670,581
SEP	124	1,101,735
TOTAL YTD	1,291	281,451,400

*As of 9/30/2021





Compromises by Sector Q3 21 vs. Q3 20 & Q3 19						
Sector	Year					
	Q3 2021		Q3 2020		Q3 2019	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	25	463,043	11	41,305	13	3,699,122
Financial Services	69	1,649,306	25	793,960	30	100,150,121
Government	21	1,427,008	9	507,031	16	136,336
Healthcare	78	7,042,068	55	1,535,813	90	2,807,590
Hospitality	5	31,069	5	17,067,862	8	154,959
Manufacturing & Utilities	48	48,294,629	18	513,371	14	31,698
Military						
Non-Profit/NGO	21	94,615	10	13,079	12	185,823
Professional Services	49	1,532,452	31	308,194	18	35,048
Retail	21	520,028	14	9,679,279	23	284,538,181
Technology	12	406,007	18	20,253,547	7	430,685
Transportation	8	97,484	4	11,636	4	16,996
Other	87	63,577,823	48	10,121,823	29	1,824,477
Unknown	1 (Unknown – marketing database)	35,000,000				
TOTALS:	445	160,135,532	248	60,846,900	264	394,011,036





**IDENTITY THEFT™
RESOURCE CENTER**
21 Years of Service

Attack Vector 2021 YTD vs. Full Years 2020 & 2019			
Attack Vector	2021 YTD	2020	2019
Cyberattacks	1,111	878	928
Phishing/smishing/BEC	370	383	490
Ransomware	244	158	83
Malware	103	104	112
Non-secured Cloud Environment	19	50	15
Credential Stuffing	12	17	3
Unpatched software flaw	2	3	3
Zero Day Attack	2	1	n/a
Other - not specified	359	162	222
System & Human Errors	134	152	231
Failure to configure cloud security	48	57	56
Correspondence (email/letter)	40	55	89
Misconfigured firewall	9	4	4
Lost device or document	7	5	19
Other - not specified	30	31	63
Physical Attacks	35	78	118
Document Theft	3	15	19
Device Theft	12	30	57
Improper Disposal	3	11	14
Skimming Device	N/A	5	4
Other - not specified	17	17	24
Unknown	11	N/A	2
TOTALS:	1,291	1,108	1,279





Compromises by Sector Q3 21 vs. Q3 20 & Q3 19						
Sector	Year					
	Q3 2021		Q3 2020		Q3 2019	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	25	463,043	11	41,305	13	3,699,122
Financial Services	69	1,649,306	25	793,960	30	100,150,121
Government	21	1,427,008	9	507,031	16	136,336
Healthcare	78	7,042,068	55	1,535,813	90	2,807,590
Hospitality	5	31,069	5	17,067,862	8	154,959
Manufacturing & Utilities	48	48,294,629	18	513,371	14	31,698
Military						
Non-Profit/NGO	21	94,615	10	13,079	12	185,823
Professional Services	49	1,532,452	31	308,194	18	35,048
Retail	21	520,028	14	9,679,279	23	284,538,181
Technology	12	406,007	18	20,253,547	7	430,685
Transportation	8	97,484	4	11,636	4	16,996
Other	87	63,577,823	48	10,121,823	29	1,824,477
Unknown	1 (Unknown – marketing database)	35,000,000				
TOTALS:	445	160,135,532	248	60,846,900	264	394,011,036

METHODOLOGY NOTES: For purposes of quarterly and annual reporting, the ITRC aggregates data events based on the date the breach, exposure, or leak was entered into the database rather than the date the event occurred. This avoids the confusion and data conflicts associated with the need to routinely update previous reports and compromise totals. The date of the original compromise, if known, and the date of the event report are noted in the ITRC's *notified* data compromise tracking database.

The number of victims linked to individual compromises are updated as needed and can be accessed in the ITRC's *notified* breach tracking solution.

The ITRC reports Third-Party/Supply Chain Attacks as a single attack against the company that lost control of the information. The total number of individuals impacted by third-party incidents is based on notices sent by the multiple organizations impacted by the single data compromise.

Unless otherwise noted, all data reported on October 6, 2021, as entered through September 30, 2021.

FOOTNOTES:

¹ Data exposures are not generally not data breaches under the ITRC's definition. Generally, a Data Exposure means personal information was accessible by unauthorized people, but there is no evidence the information was viewed, copied, or removed from the database where it is stored. A data exposure carries a lower risk of identity theft or fraud.

² The number of data compromises has been adjusted as part of a data audit.

³ *University of Michigan: Data breaches – Most victims unaware when shown evidence of multiple compromised accounts*

⁴ *Carnegie Mellon University: After a breach, users rarely change their passwords, and when they do, they're often weaker*



Exhibit B

2021 CONSUMER AFTERMATH® REPORT

How Identity Crimes Impact Victims,
their Families, Friends, and Workplaces



ITRC IDENTITY THEFT
RESOURCE CENTER
21 Years of Service

idtheftcenter.org • 1-888-400-5530

Letter from the CEO



Eva C. Velasquez
(President & CEO, ITRC)

"It is not resolved." Out of all the responses to this year's Identity Theft Resource Center Consumer Aftermath survey, this is the answer that hurts my heart and angers me the most. Our 2021 victim impact study you are about to read captures the emotional, physical, and lost opportunities of identity crime victimization, just as our previous reports have done.

While everyone is living through the effects of the COVID-19 pandemic, identity crime victims have the additional challenge of resolving issues created by someone misusing their personal information. Some of the identity fraud victims we assist have jobs, and stable housing, and are better equipped and resourced to face the challenges of having your identity stolen that have become all too common. Many more, though, are the people most in need of critical relief dollars they cannot collect because a criminal has fraudulently applied for funds in their name.

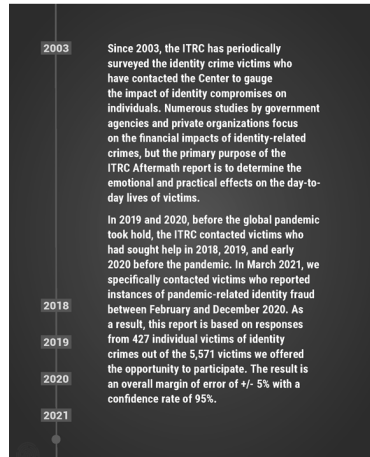
These are not folks who are missing out on fun on activities, or "extras" while they jump hurdles to reclaim their identities. They cannot pay their rent or mortgage. They cannot put food on the table or gas in their cars. They cannot afford to pay for internet access or child-care needed to look for new employment. You will see the range of emotions – anger, frustration, fear, hopelessness – in their own words.

We talk to victims every day. In fact, more people than ever are reaching out to us for one-on-one victim assistance and education as a result of a dramatic increase in identity fraud and a shrinking set of resources. The statements you are about to read from the very people that are being harmed make a convincing case as to why we need government agencies, private companies, and charitable foundations to increase the funding available to help victims of identity crimes.

But that is not the course we are charting today. The US Department of Justice has not funded any program aimed at helping identity crime victims in eight of the last 10 budget cycles, including 2019, 2020, and to-date in 2021. That's despite a nearly 250 percent increase in identity fraud reported to the FTC – from 400,000 in 2016 to more than 1.3 million last year – and a 2x increase in the number of identity crimes reported to the FBI over the same time period.

Without increased financial support from all Public, Private, and Non-profit stakeholders, free victim services like those provided by the ITRC will soon be reduced or disappear. "It was not resolved" today could turn into "it will never be resolved" tomorrow. Join us and other leading organizations in making the victims of identity crimes a priority.

May 2021



We opted to expand our normal data set and time frame because of the pandemic. When states began to issue shelter-at-home orders, the ITRC Contact Center staff immediately noticed trends that indicated a rapid rise in identity fraud, especially in government benefits programs. Government and private data show the scope of the identity fraud linked to pandemic relief benefits - especially unemployment benefits - but there has been little information about the effects of identity fraud on the victims who have been denied needed benefits.



The information presented here shows both the scale and the insidious nature of pandemic-related identity crimes.

We contacted 752 identity crime victims who previously self-identified as being impacted by pandemic-related identity fraud at the time they contacted the ITRC in 2020. We received 63 responses for a margin of error of +/- 12 percent with a confidence level of 95%.

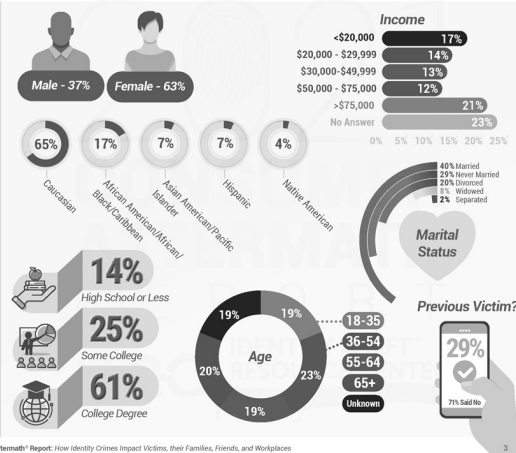
© 2021 ITRC Consumer Aftermath® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

2

Demographics

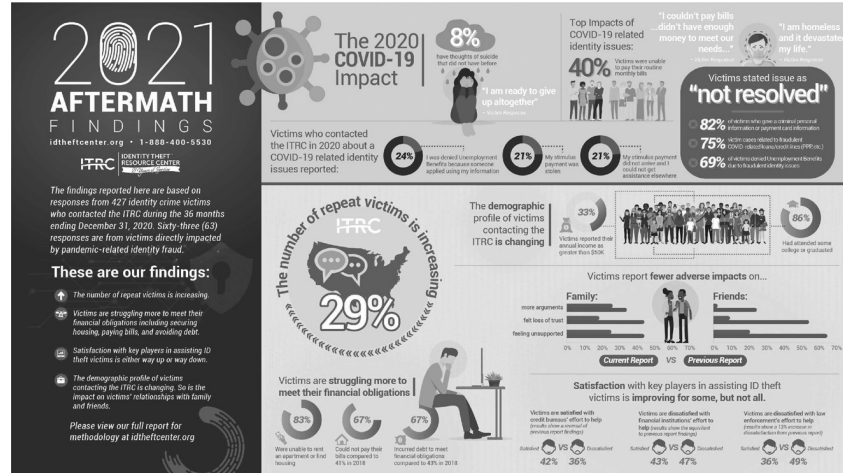
The profile of a "typical" identity crime victim who contacts the ITRC is remarkably consistent in most key demographics. Victims are primarily married women spread evenly across all adult age groups. The number of victims who self-report low annual income nearly matches the number of victims who report high annual earnings.

However, victims with college degrees contact the ITRC for assistance far more frequently than victims who do not have degrees. In terms of race and origin, victims skew higher than the US population among White non-Hispanic, African-American, and Native American populations, but slightly lower among Asian Americans / Pacific Islanders and significantly lower among victims of Hispanic origin.

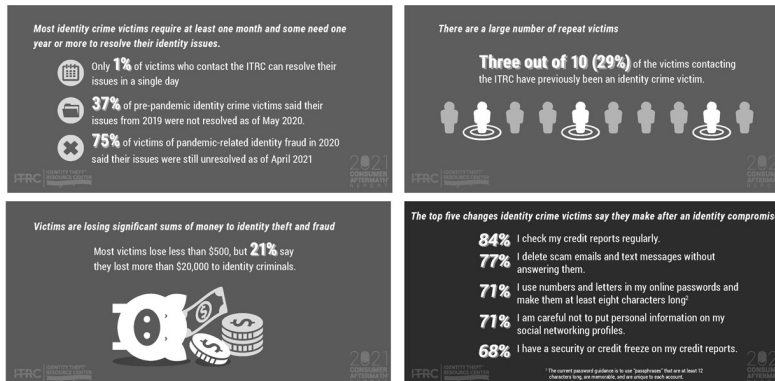


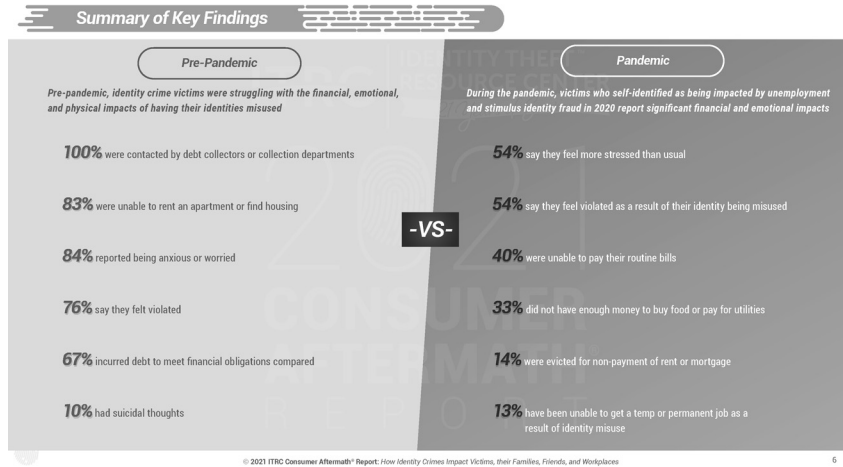
© 2021 ITRC Consumer Aftermath® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

3



Summary of Key Findings





Impacts of COVID-19 Pandemic Related Identity Crimes

In 2019 the number of contacts to the ITRC about unemployment benefit fraud totaled .00019% of all contacts. In 2020 that number jumped to eight percent (8%) thanks to the COVID-19 pandemic. The impacts of government benefit related identity fraud can be severe and long-term as illustrated in the responses from 63 pandemic related identity fraud victims who contacted the ITRC in 2020.



© 2021 ITRC Consumer Alternatives® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces 7

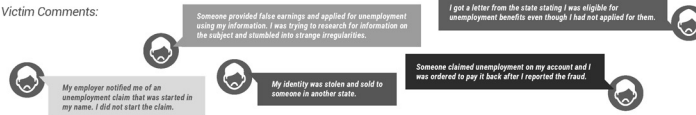
Question #1

Top Responses

You contacted the ITRC in 2020 about a COVID-19 related identity issue. Please select one or more of the following topics:

- ☐ I was denied Unemployment Benefits because someone applied using my information 24%
- ☐ My stimulus payment was stolen 21%
- ☐ My stimulus payment did not arrive and I could not get assistance elsewhere 21%
- ☐ I received Unemployment Benefits, but I did not apply for them 14%
- ☐ I received one or more unsolicited Unemployment Benefits payment cards at my home address 5%
- ☐ Someone applied for a Paycheck Protection Program (PPP), Small Business Administration Loan, or other credit in my name 5%
- ☐ I received a Form 1099-G saying I owed taxes on Unemployment Benefits I did not apply for or receive 3%
- ☐ I fell for a COVID-related scam where I gave someone my bank account or payment card information 3%
- ☐ I fell for a COVID-related scam where I gave someone my personal information like a login or password 2%

Victim Comments:



© 2021 ITRC Consumer Alternatives® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

8

Question #2

Top Responses

If you were denied Unemployment Benefits how long did it take to resolve the issue? (data reflects 21% of total respondents)

- ☐ It is not resolved 69%
- ☐ Less than seven days 21%
- ☐ Six to nine months 15%
- ☐ Three to six months 8%
- ☐ One to four weeks 8%

Question #3

If someone applied for COVID-related loans/credit lines (Examples: a PPP Loan or Small Business Administration EID Loan) with your identity information; or, if you gave a criminal your personal information or payment card information as part of a phishing or other scam, how long did it take to resolve the issue? (38% of total respondents)

- ☐ It is not resolved 75%
- ☐ Less than seven days 38%
- ☐ One to four weeks 13%
- ☐ Three to six months 8%
- ☐ Six to nine months 4%

© 2021 ITRC Consumer Alternatives® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

9

Question #4

Top Responses

If you gave a criminal your personal information or payment card information, how long did it take to resolve the issue?

(27% of total respondents)

- It is not resolved **82%**
- Less than seven days **27%**
- Three to six months **12%**
- One to four weeks **6%**



Share this! ➔

© 2021 ITRC Consumer Aftermath® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

10

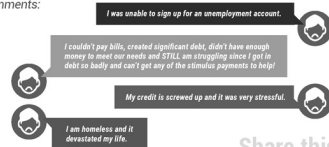
Question #5

Top Responses

What financial impact did these COVID-19 related identity issues have on you?

- I was unable to pay my routine monthly bills **40%**
- I did not have enough money to buy food or pay utilities **33%**
- No impact **22%**
- I was evicted for failing to pay rent or mortgage **14%**
- I could not make my car payment **14%**
- I could no longer afford child or elder care **8%**

Victim Comments:



Share this! ➔



© 2021 ITRC Consumer Aftermath® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

11

Question #6

Top Responses

What non-financial impacts did these COVID-19 related identity issues have on you?

I feel more stressed than usual	54%
I feel violated as a result of my identity being misused	54%
I feel helpless or powerless as a result of my identity being misused	43%
I feel more frustrated or annoyed than usual	41%
I trust people less as a result of my identity being misused	37%
I argue more often with my friends and/or family than usual	19%
I have been unable to get a temporary or permanent job as a result of my identity being compromised	13%
I have thoughts of suicide that I did not have before	8%
No impact	8%

Victim Comments:



I've always been poor, but this entire year long problem has made my life a living nightmare!



I am ready to give up all together

© 2021 ITIC Consumer Alternatives® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

12

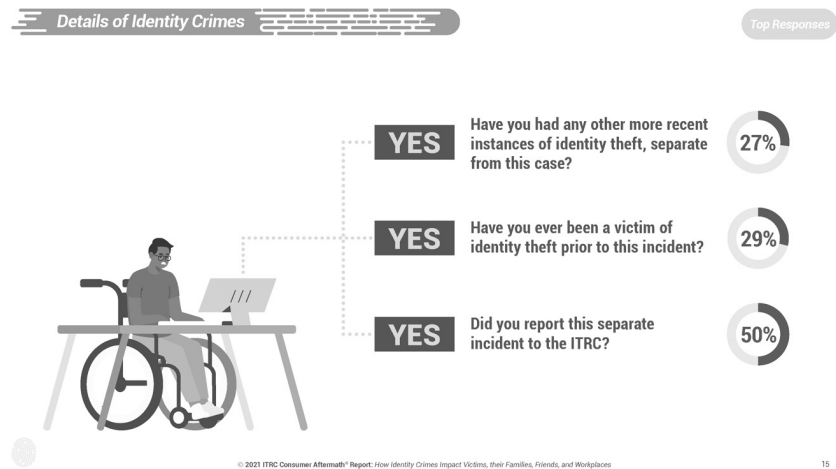
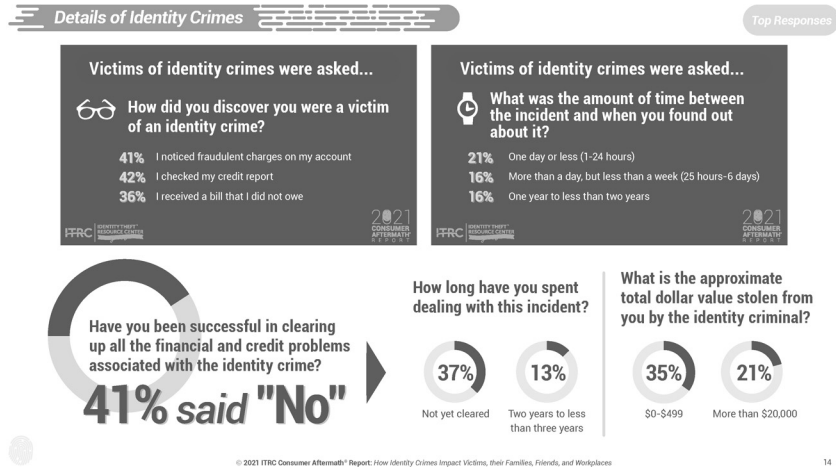
Impacts of Pre-Pandemic Identity Crimes

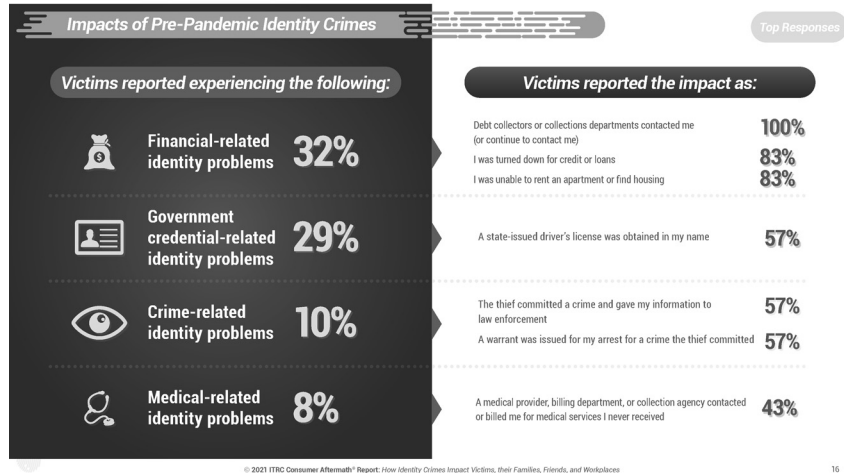
The following pages are the **TOP RESPONSES** to select questions from 362 identity crime victims. For complete responses, please visit idtheftcenter.org



© 2021 ITIC Consumer Alternatives® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

13

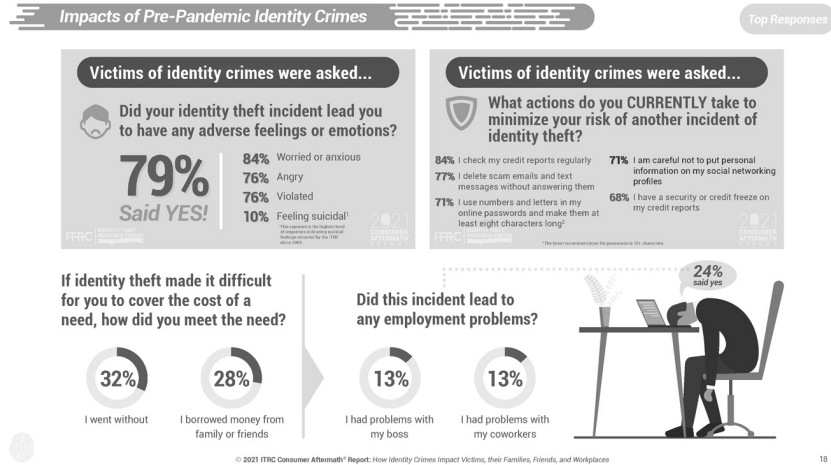




16

Share this! © 2021 ITRC Consumer Alternatives® Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces

17



18



19



2021 CONSUMER AFTERMATH® REPORT



Acknowledgements

This report was created based on responses from identity theft victims obtained using tools from Development Services Group, Qualtrics, and MailChimp.

Consumer & Business Resources

For more information about the free services and education opportunities for consumers as well as fee-based services for businesses, visit idtheftcenter.org or by email.

communications@idtheftcenter.org



EXHIBIT C

The information for Exhibit C can be found on the Identify Theft Resource Center website under the “2021 Consumer Aftermath Report” (idtheftcenter.org).

The CHAIR. Thank you, Mr. Lee. And again, thank you for your annual reports and the information that you provided to the Committee. I don't even know if in the Q&A I will get to ask all my questions about that, but I am interested in the State rankings. And you have data that shows the—what is going on in each state. So I think that that is also interesting data for our committee members. So thank you. Ms. Rich, welcome. Thank you for being here.

**STATEMENT OF JESSICA L. RICH, OF COUNSEL, KELLEY DRYE
& WARREN; DISTINGUISHED FELLOW, GEORGETOWN
INSTITUTE FOR TECHNOLOGY LAW AND POLICY**

Ms. RICH. Chair Cantwell, Ranking Member Wicker, and members of the Committee, I am Jessica Rich, a counsel at Kelley Drye & Warren, and also a distinguished Fellow at Georgetown Law. I am pleased to be here today testifying on the need to strengthen data security protections in this country.

My remarks today are my own based on my years in Government service. And my background is as a lawyer and a law enforcement official. I worked for 26 years at the Federal Trade Commission, the last four as its director of Bureau of Consumer Protection. Before becoming the Director, I was the first and longtime manager of the FTC's privacy program. I have supported stronger data privacy and security laws for over 20 years. Providing reasonable security for consumer data is at the heart of privacy protection.

Without it, data can easily be stolen or compromised by hackers or corrupt insiders. And that is what we have seen again and again, scores of data breaches that harm consumers and businesses alike in the form of fraud and identity theft, loss of trust, and business disruption. Because commercial systems are highly connected to the Nation's infrastructure, these compromises undermine our national security as well. One of the key problems is that current law fails to set clear standards for data security or provide adequate remedies. Most of the FTC's data security efforts are based on the FTC Act, a law that leaves wide gaps in protection and doesn't even authorize penalties for first time violations.

While there are sector specific laws with a data security component and half the states now have their own data security laws, it is a messy and confusing patchwork. For all of these reasons, I strongly support Federal data security requirements, whether it is part of a broader privacy law or on its own, if that can be done, to bring stronger protections and greater clarity to the marketplace.

My written remarks detail the main elements I recommend in such a law, so many of which are already contained in some form in both the Chair's and the Ranking Member's privacy bills. The convergence between these bills reflects hard work and commitment by this committee and shows that a Federal data security standard is truly within reach. The Committee's efforts to create a new privacy bureau at the FTC, something I have also personally championed, will also make an enormous difference for data protection in this country. So in terms of the elements. First, the law should provide comprehensive protections and a level playing field across the marketplace.

This means giving the FTC jurisdiction over nonprofits and common carriers, which they don't currently have jurisdiction over. Second, it should take—the law should take a process based approach that is scalable to different types and sizes of companies and the volume and sensitivity of the data they collect. Otherwise, the law could quickly become obsolete or impose requirements ill-suited and unattainable for small businesses. And there should be requirements or incentives for data minimization, as my fellow panelist just discussed.

Third, the law should extend broadly to the wide range of data that in the world of AI and algorithms and IoT and sophisticated consumer profiling can cause consumer privacy harm. This means data that is reasonably linkable to a consumer, and categories of data that go well beyond Social Security and account numbers, like account credentials, health data not covered by HIPPA, and precise geolocation data.

Fourth, to ensure accountability and deterrence, the law should authorize strong remedies, both civil penalties and redress, require oversight by qualified personnel reporting to the highest levels of the organization, and give full enforcement authority not just to the FTC, but to the state Attorneys General. Finally, if the law is really strong enough and the states can fully enforce it, I don't think we weaken protections at all by preempting State laws and foregoing a private right of action.

In fact, we gain a strong, consistent standard that can be enforced nationwide by over 51 law enforcement agencies working in tandem. However, given the chasm that continues to exist on private rights of actions in particular, there are middle grounds to consider as I discuss in my written testimony. Thank you for having me here today and I am happy to answer questions.

[The prepared statement of Ms. Rich follows:]

PREPARED STATEMENT OF JESSICA L. RICH, OF COUNSEL, KELLEY DRYE & WARREN;
DISTINGUISHED FELLOW, GEORGETOWN INSTITUTE FOR TECHNOLOGY LAW AND
POLICY

I. INTRODUCTION AND BACKGROUND

Chair Cantwell, Ranking Member Wicker, and members of this Committee, I am Jessica Rich, Of Counsel at Kelley Drye & Warren and a Distinguished Fellow at Georgetown University. I am pleased to be here today, testifying before this Committee on the need to strengthen data security protections in this country. I want to thank this Committee for its leadership and ongoing efforts on data privacy and security issues. I also want to make clear that my remarks today are my own, based largely on my years of experience in government service.

My background is as a lawyer and law enforcement official. I worked for over 26 years at the Federal Trade Commission (FTC), the last four as Director of its Bureau of Consumer Protection overseeing the agency's fraud, advertising, and privacy initiatives. Earlier in my FTC career, I launched the agency's very first privacy work, and then led and expanded these efforts for over a decade—bringing cases against companies that misrepresented their privacy practices and/or failed to secure consumer data, and developing rules to implement the Gramm Leach Bliley Act (GLB),¹ Children's Online Privacy Protection Act (COPPA),² and Fair and Accurate Credit Transaction Act.³ In 2000, I led the FTC team that wrote the first of many reports to Congress⁴ seeking stronger legal authority and remedies for data privacy and security—and I have testified, spoken publicly, and written many articles pleading the same case since.

Providing reasonable security for consumer data is at the heart of privacy protection. Even if a company determines not to sell or share its data with anyone, data can still be stolen through the proverbial “back door” if it is not protected from hackers or insiders with ill-intent.

And that is what we have seen, again and again over the years—scores of data breaches that harm consumers and businesses alike.⁵ For consumers, data security failures can lead to fraud and identity theft, and the expense and worry of moni-

¹ 15 U.S.C. § 6801 et seq.

² 15 U.S.C. § 6501 et seq.

³ 15 U.S.C. § 1681 et seq.

⁴ <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

⁵ See e.g., <https://www.upguard.com/blog/biggest-data-breaches>.

toring compromised accounts, changing passwords, and recovering losses.⁶ For businesses, data security lapses can lead to loss of trust among customers, lost business, costly remedial efforts, and ransomware and other serious disruptions to operations.⁷ Because commercial systems are highly connected to the Nation's infrastructure, these compromises can undermine our national security as well.⁸

One of the problems is that current law fails to set clear and consistent standards for data security, or provide a solid basis for holding companies accountable. Indeed, most of the FTC's data security efforts are based on the FTC Act,⁹ a law that was not designed for this purpose and is ill-suited for it in many ways. Among other things, the law does not establish clear standards for everyone to follow before problems occur—it is largely reactive. It does not cover non-profits, or companies engaged in common carrier activities. It does not authorize civil penalties for first time violations.

And now, after the Supreme Court's ruling in the *AMG* case,¹⁰ the law does not even allow the FTC to seek monetary relief in Federal court under Section 13(b).

While the FTC has some authority over data security under certain sector-specific laws (Fair Credit Reporting Act,¹¹ GLB, and COPPA), these laws cover small slivers of the marketplace. Further, half of the states have now passed data security laws of their own, splintering the issue even further.¹²

The absence of Federal standards in this area means that businesses lack clear rules to follow; consumers lack consistent and reliable protections, and remain confused and distrustful; and the FTC turns somersaults and faces legal challenges as it tries to fill the gaps. For all of these reasons, the U.S. urgently needs a Federal standard that would bring stronger protections and greater clarity to the marketplace.

II. KEY QUESTIONS IN THE DATA SECURITY DEBATE

As this Committee is well aware, despite growing support for the *concept* of a Federal data security law, many questions and disagreements remain about what it would include. So, to get right to the point, I offer my thoughts (below) on some key questions that always arise when the prospect of a Federal data security law is discussed.

Should data security be addressed in a standalone Federal law or as part of a Federal privacy law? Including data security as part of a Federal privacy law has the advantages of ensuring that privacy and data security requirements are harmonized; that consumers gain comprehensive protections all at once; and that companies can move forward with compliance plans on both fronts. Nevertheless, passing a data security law on its own would still advance data protection in this country considerably.

Who should enforce a Federal data security law? The FTC, at the Federal level. It has deep background and expertise in this area from over 20 years of enforcement experience and policy leadership; a strong commitment to the issue, and relationships with key sister agencies here and abroad (the Department of Justice, Health and Human Services, and international privacy enforcers and regulators, among others). With enhanced legal authority, the FTC could hit the ground running in a way no other agency could (and certainly not a brand new one). Providing the FTC with additional resources (the topic of last week's hearing) would also be critically important.

As discussed below, the State Attorneys General also should be fully empowered to enforce the Federal law.

What elements should be included in such a law? The new law should fill many of the gaps discussed above:

First, it should extend across the marketplace to provide comprehensive protection to consumer and a level playing field to businesses. This means giving the FTC jurisdiction over non-profits and common carriers.

Second, the law should extend broadly to any data that, if not protected, could be used to cause consumer harm. In particular, the law should cover data that is

⁶See e.g., https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

⁷See e.g., <https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses>.

⁸<https://www.cisa.gov/critical-infrastructure-sector-partnerships>.

⁹<https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act-ftc-act-incorporating-us-safe-web-act.pdf>.

¹⁰https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.

¹¹15 U.S.C. § 1681 et seq.

¹²<https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>.

reasonably *linkable* to a consumer, and should include categories of data that go well beyond account numbers—e.g., account credentials, health data not covered by the Health Insurance Portability and Accountability Act,¹³ and precise geolocation data.

Third, the law should provide clarity about companies' obligations while also giving them flexibility to tailor their data security protections to their business models. This means taking a process-based approach that includes certain key elements: (1) regular risk assessments (2) effective safeguards to limit the risks (3) a data security plan that is socialized throughout the company (4) training and oversight of employees and vendors (5) regular evaluation and updates to the plan and safeguards, and (6) accountability and oversight by expert personnel who report to the highest levels of the company. In addition, there should be requirements or incentives for companies to minimize unnecessary data collection and storage, as this is a huge source of risk to data.

Finally, of critical significance, the law should include the authority for the FTC (and the states) to obtain civil penalties and (in light of the *AMG* ruling) consumer redress—to deter misconduct and compensate consumers for their losses.¹⁴

Does a process-based approach provide sufficient guidance to companies as to their obligations? This question has been a source of debate. Companies have sometimes argued that they want more specific guidance, even as they also say they want flexibility. To address this concern, the Federal law could direct the FTC to issue periodic guidance providing detailed, up-to-date information regarding security measures and technologies that companies should consider adopting. The guidance would not itself be enforceable, but it could provide valuable information that could be updated on a regular basis.

Does the FTC need rulemaking to implement a Federal data security law? A key purpose of rulemaking is to ensure that a law keeps pace with rapid technological and market changes. Here, if the law takes a process-based approach and also directs the FTC to issue periodic guidance, full rulemaking authority may not be necessary. However, there may be specific issues for which rulemaking is needed—notably, what type of data should be covered under the law, an important issue that is likely to evolve over time.

Should the law preempt state laws in this area? Preemption has the advantage of ensuring clarity and consistency in an area that, as here, is already complex and costly. On the other hand, the states have shown leadership in this area and their continued efforts could help strengthen protections and accountability nationwide. A good middle ground would be to preempt state data security laws while fully empowering the states to enforce the Federal law. The law could provide a mechanism for coordination, similar to the coordination provisions in COPPA.

Should the law grant a private right of action? Ideally, a private right of action should not be necessary. One of the main arguments in support of a private right of action is that the FTC, with its limited resources, cannot possibly police the marketplace adequately to promote compliance, deter wrongdoers, and obtain recourse for injured consumers. A strong Federal law could address these concerns by giving the FTC the legal tools and resource it needs, empowering the states to enforce the Federal law, and including strong remedies for violations.

Federal and state enforcement—with no private right of action—would also facilitate more consistency, and prevent the types of class actions that have benefited lawyers more than consumers.

However, stakeholders have debated this issue for decades with no resolution. To bridge the divide, Congress could consider some middle-ground options—something Cam Kerry at Brookings¹⁵ and others have written about. For example, a private right of action could be limited to willful and repeated violations and/or actual damages. It also could require proof of tangible harm, such as when data security failures result in fraud or identity theft; indeed, the recent Supreme Court decision in *Trans Union*,¹⁶ which defined privacy injury fairly narrowly for purposes of standing in private actions, may already have compelled this outcome. Additionally, a private right of action could be subject to a right to cure, as in California's privacy law,¹⁷ but that right would need to be clearly defined.

¹³<https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>.

¹⁴I did not include breach notification in these recommendations. With state breach notification laws now in effect in all 50 states, I believe including this issue would be highly disruptive to the goals of passing Federal data security legislation.

¹⁵<https://www.lawfareblog.com/privacy-legislation-private-right-action-not-all-or-nothing-proposition>.

¹⁶https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.

¹⁷https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.815.

III. CONCLUSION

I would be happy to assist the Committee as it continues its work on this important issue. Thank you for allowing me to share my views today.

The CHAIR. Thank you, Ms. Rich. Mr. Felten, Professor Felten, is that right?

Mr. FELTEN. Yes, thank you.

The CHAIR. Thank you very much for being here and thank you for your work.

**STATEMENT OF EDWARD W. FELTEN, ROBERT E. KAHN
PROFESSOR OF COMPUTER SCIENCE AND PUBLIC AFFAIRS,
PRINCETON UNIVERSITY; FORMER CHIEF TECHNOLOGIST,
FEDERAL TRADE COMMISSION**

Mr. FELTEN. Thank you. Chair Cantwell, Ranking Member Wicker, and distinguished members of the Committee, thank you for the opportunity to testify today. I am testifying today in my personal capacity. A few years ago, researchers discovered that many widely sold webcams had been set up by their manufacturers with weak passwords like admin, guest, and 1234.

Anyone who knew or guessed these passwords could control the camera. The consequence was that many Americans had webcams in their homes that could be turned on and viewed across the Internet by bad actors. Then a group of hackers automated the process of scanning the Internet for vulnerable webcams and installing malware on them.

By doing this, they took control of hundreds of thousands of devices all over the internet, and they operated those compromised devices under centralized control in what was dubbed the Mirai botnet. Mirai was used to launch some of the largest denial of service attacks seen to that time, including one against an infrastructure provider that knocked many sites offline for hours. It knocked out Twitter, Reddit, and Netflix, among others.

A single and simple, careless practice had led to a cascade of harm. And there was little that consumers could have done to protect themselves. The FTC later brought enforcement action against D-Link, a prominent webcam maker, requiring it to change its practices. My written testimony summarizes another similar case, and I could have included many more. It is a distressingly common story. Consumers unable to protect themselves rely on a company to take adequate precautions. The company fails to do so. Intruders exploit that failure. Consumers are harmed. And an FTC enforcement follows.

I had the privilege of serving as the FTC's first Chief Technologist about 10 years ago. The FTC's staff and leadership were and are smart, diligent, and dedicated to protecting consumers, but they simply don't have the tools they need to fully address today's data security enforcement challenges. I would respectfully suggest three steps that Congress might take to further empower the FTC. First, as others have advocated, Congress can allow civil penalties for first time violations of Section 5 of the FTC Act. The lack of first time penalties makes the FTC Act a weak deterrent and attempts a company to gamble that it won't face enforcement, or if it does, it can go ahead with unfair practices and then clean up its act after the first enforcement.

For example, D-Link paid no penalties in the FTC's webcam enforcement. A second step Congress might take is to authorize a data security rulemaking so the FTC can clarify what is expected of companies. Today, most enforcements rely on Section 5, which is broad but not specific.

The FTC has created a body of case law through its enforcement and public statements, but more specificity would better protect consumers and help companies better understand what is expected of them. A good structure would cover both internal controls and responsibility, in the spirit of the GLBA safeguard rule, and also require basic best practices that are already widespread at well-managed companies, such as keeping up to date on security patches.

My written testimony offers a longer list of suggested provisions. A third step Congress might take is to increase the FTC's resources for data security and technology, and to create a new technology focused bureau in some form. When I joined the FTC in 2011 as its first Chief Technologist, the agency was just starting to build its workforce of technologists. The need for more technology expertise was clear. And although the FTC has increased its capacity to hire and work with technologists over the 9-years since my term ended, there is still a long way to go.

Government can't match the salaries or working conditions available to top technologists in the private sector. But the FTC can find and recruit outstanding technologists who are motivated by the agency's mission of protecting Americans. I know these motivated technologists exist because I have met many of them and helped some of them get jobs at the FTC.

Skilled technologists will come to the FTC, and they will stay as long as they believe they are empowered as full partners in fulfilling the agency's mission. This requires building a community of practice and establishing career paths for technologists in the FTC so that they can develop their talents and can hope to rise to high levels in the agency staff if their performance merits it.

The key is to activate the virtuous cycle, where successful recruiting increases the team's impact on the mission, and the impact on the mission attracts top talent to join the team. The successful FTC of the future is one that has stronger authority, increased resources, and greater technological capability. The FTC is ready to grow into this role, and I thank the Committee for your work on empowering the FTC to do this on behalf of American consumers. Thank you for your time and I look forward to your questions.

[The prepared statement of Mr. Felten follows:]

PREPARED STATEMENT OF EDWARD W. FELTEN, PROFESSOR OF COMPUTER SCIENCE
AND PUBLIC AFFAIRS, EMERITUS, PRINCETON UNIVERSITY

Chair Cantwell, Ranking Member Wicker, and distinguished members of the Committee, thank you for the opportunity to testify.

As you know, data security is an issue that is important to many Americans. More and more data about our lives is captured, stored, and analyzed, with little transparency about what is collected, who has it, what they are doing with it, and how well companies are protecting it. Even the most careful companies may be subject to a data breach, and of course the existence of a breach does not by itself prove security measures were inadequate. But too often companies fail to take common, reasonable steps to ensure data security, and too often these failures lead to breaches that ultimately harm consumers.

At the national level, the Federal Trade Commission plays a primary role in civil enforcement to protect data security in most sectors of the economy, mainly by enforcing Section 5 of the FTC Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.”

I had the privilege of serving as the FTC’s first Chief Technologist from 2011–2012, and I have continued to follow the FTC’s data security activities since. My testimony is informed by these experiences and by my academic study of data security and privacy from both technical and policy perspectives. I am testifying in my personal capacity and not on behalf of any agency or organization.¹

In this testimony I will cover two main areas. First, I will summarize two examples in which companies’ data security failures led to breaches that harmed consumers. Second, I will discuss three things Congress might do to strengthen the FTC’s ability to protect consumers: enabling civil penalties for first violations of the FTC Act; creating a statutory or rulemaking framework regulating data security practices; and providing resources to grow and empower the FTC’s technology workforce.

Impact on Consumers: An Example

The following example helps illustrate how data security failures put Americans at risk.

Over the last decade or so, cheap Internet of Things devices have proliferated in our homes and offices. For example, a parent might set up a webcam in their home and then, while on a family trip to visit relatives, might use a phone app to turn on the webcam and verify that all is well back at home. This requires a way for the parent’s phone to connect over the network to the webcam and send a command to the camera to stream video back to the parent’s phone. Security requires that the webcam must only accept commands from the authorized phones of the parents and not from other sources.

In 2015, research revealed that many widely sold webcams had hidden administrative functions that allowed anyone to log in to the webcam and control it from afar, using weak and widely known username/password combinations such as admin/admin, guest/guest, and administrator/1234. These were not weak passwords chosen by the consumer but rather passwords set up in advance by the manufacturer, without notice to the consumer and without any reasonable way for the consumer to change them.

The consequence was that many Americans had webcams in their homes and offices that could be turned on and viewed across the Internet by bad actors.

In addition to enabling direct exploitation to spy on consumers, these vulnerabilities also opened the door to attackers using webcams as a jumping-off point for cyberattacks on other targets anywhere on the Internet.

This very possibility was exploited by hackers who automated the process of scanning the Internet for vulnerable webcams and similar devices, and installing malware on them. By this means they took control of hundreds of thousands of devices all over the Internet, and operated those compromised devices under centralized control to form what was dubbed the Mirai botnet. Discovered in 2016, Mirai was used to launch some of the largest denial of service attacks seen to that time, including one against an infrastructure provider that knocked many sites, including Twitter, Reddit, and Netflix, offline for several hours. Three young Americans would later plead guilty to these crimes.²

There was little if anything that consumers could have done to protect themselves. Nothing on the webcams or their packaging suggested the existence of a minimally protected administrative interface. Few consumers would have had the technical know-how to check or probe the devices themselves. Consumers should have been able to rely on companies to take simple and reasonable precautions to ensure data security.

Consequences of Weak Security: The Equifax Breach

Even large and well-known companies sometimes fail to protect the security of consumer data.

In 2017 the consumer credit reporting company Equifax discovered a series of intrusions into its systems through which the private data of about 150 million people was extracted—including 145 million unencrypted social security numbers. The FTC

¹Although I am a Member of the Privacy and Civil Liberties Oversight Board, I am testifying solely in my individual, non-official capacity.

²More detail about these events is available from the U.S. Department of Justice: *Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant Cyber Attacks*, Dec. 13, 2017. <https://www.justice.gov/usao-nj/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases>

and other agencies investigated, and Equifax ultimately agreed to a consent order including penalties of about \$600 million.

According to the FTC and other sources, the initial breaches occurred because the company failed to apply an available security patch to a component of one of its public-facing servers. The company knew of the problem—the security flaw in the component—and also knew of the availability of the solution—the security patch—but still failed to apply the patch to all of its vulnerable systems. Multiple intruders exploited this failure and gained unauthorized access to Equifax systems.

Because the company did not take other precautions, such as partitioning its network, intruders were able to move laterally from the initially compromised system into other internal Equifax systems. Compounding this failure, the first breached system had access to an unprotected, unencrypted file share that listed administrative passwords for internal systems in plain text, which further helped the intruders expand their access.

The intrusions went undetected for about four months, in part because the company was not consistently using common defensive measures such as file integrity checking and network intrusion detection.

Several of these failures, such as neglecting to apply security patches and storing sensitive data in unencrypted form, were contrary to the company's own internally stated policies, suggesting a broader failure to oversee and manage its internal data security operations. The company's settlement with the FTC required it to establish stronger data security management and accountability structures.

As in the webcam example, there was little if anything that consumers could have done to protect themselves. Equifax, as a consumer credit reporting agency, has data on many Americans who are not its customers, and even those who are customers of an Equifax service would have had no visibility into the company's internal security practices or policies. The affected people could only rely on the company to adopt reasonable measures, and on the FTC and other enforcement bodies to enforce the law when necessary.

Further Empowering the FTC to Protect Data Security

The FTC's staff and leadership have been diligent and dedicated to their data security mission. Yet the agency has sometimes struggled to cope with the sheer scope, scale, and complexity of this mission—and these challenges will only become more difficult as digital technologies continue to proliferate and become even more complex.

Based on my experience at the FTC and my study of the agency, I would point to several factors, listed below, that have contributed to these challenges.

Limitations of the FTC Act: No Civil Penalties for First-time Violations

A first challenge has been the structure of the FTC Act. Section 5 of the Act imposes no civil penalty for a first-time violation, so even companies who commit serious violations can get a free pass if they have not faced an FTC enforcement action before. Often, the most important effect of an enforcement action is merely to enable civil penalties for subsequent violations. Furthermore, civil penalties for a second violation may only be available if the second violation involves behavior covered by the first consent order.

The combination of limited enforcement resources and no first-time penalties can make the FTC Act a weak deterrent, tempting a company to gamble that it won't face enforcement, or even if it does face enforcement, that it can gain an advantage through unfair practices and then clean up its act after the first enforcement. This opens consumers to risk. Congress could strengthen the deterrent effect of the FTC Act by authorizing civil penalties for first-time violations of Section 5, at least for data security related violations.

Many of the FTC's data security enforcements have been under the unfair practices arm of Section 5. The FTC has developed a body of case law through its past data security enforcements, and has offered guidance on some practices it considers unfair.

The case law approach has had some benefits, especially in the early days, but the public and the industry would benefit from a rulemaking that offered more specificity for companies and consumers, while retaining the flexibility needed to enable beneficial innovation in an evolving technological space. I understand that in practice, any data security rulemaking would require a new authorization from Congress.

Need for Comprehensive and Technically Focused Data Security Regulations

If Congress were to enact data security legislation that authorized an FTC rulemaking or that created a statutory framework and directed a rulemaking to fill in further details, it might include provisions such as:

- requiring companies to store and transmit sensitive consumer data in encrypted form;
- requiring strong multi-factor authentication for access to administrative accounts that can access large amounts of consumer data or can grant access to such data;
- requiring reasonable data minimization so that consumer data will be deleted when it is no longer needed for the purpose for which it was collected;
- requiring companies to apply a baseline level of security due diligence to software they build or acquire for use in handling consumer data;
- requiring companies to make reasonable efforts to track and install available security updates in systems that can access consumer data;
- where relevant and feasible, requiring companies to provide a reasonable way for consumers to get security updates for software a company supplies to them, and requiring that those updates be delivered in a secure fashion;
- in relevant cases, requiring a company to make available such security updates for a specified time period, and requiring prominent disclosure of when such security support will no longer be available;
- prohibiting companies from knowingly shipping devices or systems with serious security vulnerabilities that endanger data security;
- prohibiting companies from shipping devices or systems containing old versions of third-party software for which security patches have been issued, without a reasonable mitigation strategy;
- where a company relies on a third-party service provider to store or process consumer data, clarifying the company's responsibility to ensure that the service provider is taking reasonable steps to secure the data;
- prohibiting default settings or behaviors that put consumers at unnecessary risk;
- establishing more stringent requirements for certain sensitive categories of data such as health data, financial data, or information about children, at least when such data is outside the bounds of sector-specific privacy laws such as HIPAA, COPPA, and FERPA; and
- requiring companies handling significant amounts of consumer data to establish internal reporting and accountability structures for data security.

Need for Resources and Expertise for Technology Analysis and Enforcement

Another challenge is the limited resources available to the FTC relative to the scope of its mission—of which data security is just one small part. The limited staff and resources available for data security force the agency to be very selective and strategic in how and when it enforces the law. Companies that stay “under the radar” of the FTC may not see enforcement due to resource limits, and consumers may suffer for it.

When I joined the FTC in 2011 as its first Chief Technologist, the agency was just starting to build its workforce of technologists. The need for more technology expertise seemed clear, especially in technology-related cases. Although the FTC has increased its capacity to hire and work with technologists over the nine years since my term ended, there is still a long way to go.

Technology expertise and analysis play a crucial role in data security investigations and enforcements. Below are a few examples of how technology experts can help the FTC better protect the security of consumers' data.

- Companies that are under investigation often argue in their defense that their practices were required for technical reasons or that they chose their action over the alternatives for valid technical reasons. For instance, a threshold question in any unfairness case is whether the company's relevant behavior was unreasonable under the circumstances. Where a case depends on a company's technology design or practices, technical expertise is required to evaluate claims such as whether the company was following common engineering practices, or whether there were technically feasible alternatives and how much the alternatives would have cost in money or functionality.
- Companies also sometimes argue that they needed to collect more data, or use data more aggressively, or withhold material information about data practices from consumers in order to better protect against cyberattacks or prevent fraudulent activity by their users. Evaluating these claims, and helping enforcers understand how much cybersecurity value these measures might have provided, requires technical expertise.

- Much of the evidence in data security cases will be technological. Technology experts can understand and interpret the evidence, help to draft the Civil Investigative Demands (CIDs) used to get information from a company, and better interpret companies' responses to CIDs.
- Most investigations that lead to enforcement are resolved by a consent decree negotiated with the subject company. These consent decrees often contain forward-looking technology requirements or limitations on a company's technology practices. Technology experts can help agency leaders as they work to negotiate meaningful limits on company behavior that will continue to protect consumers as technology evolves, without unnecessarily constraining a company's ability to improve its products.

Resource limits have been one barrier to expanding the FTC's technologist workforce. Agency leaders, knowing the scope of the agency's mission and the workload facing all of its components, have found it difficult to reduce headcount elsewhere in order to hire more technologists. Congress could lower this hurdle by providing additional resources and directing some of them to building a cohort of technology experts, including people with advanced training in computer science and closely related disciplines, or with equivalent experience in industry.

How to Grow and Empower the FTC's Technology Workforce

Building and leveraging a strong technology team requires more than just a budget. Having worked as the Chief Technologist at the FTC, and having built technology teams in industry and academia, I can offer a perspective on how it might be done.

Government can't match the salaries or working conditions available to top technologists in the private sector, but the FTC can find and recruit outstanding technologists who are motivated by the agency's mission of protecting Americans. Sustaining that strategy, however, relies on keeping the implied promise that a technologist will be able to contribute fully to the agency's work, and that they can aspire to contribute more and take on more responsibility as their career advances. Retaining the best technologists will require having a career path that offers a realistic possibility of reaching the most senior staff positions in the FTC, if their performance merits it. And this will only be possible if experienced technologists are treated as full partners in the agency's internal processes and staff-level decision making, and not merely as consultants or assistants to a legal team.

Although the analogy is not perfect, an interesting comparison is to the role and organization of economists within the FTC. The Bureau of Economics has been a useful vehicle for recruiting the agency's economics workforce and applying its expertise across the FTC's missions. With technology taking on a similarly important role in the FTC's work, the question arises whether it is time to create a Bureau of Technology along similar lines. The best placement of technologists within the FTC is a point for reasonable debate; what is more certain is that the agency can benefit greatly from building up its technology team and including technologists as full partners in the agency's work across the full range of its consumer protection and competition missions.

Conclusion: The Future of Data Security, and the FTC's Role

Data security will only grow in importance as digital technology becomes more prevalent, as new technologies are invented and deployed, and as digital supply chains become more global. With more at stake, and with attackers growing in sophistication, companies need to keep improving their practices to stay ahead of the threats and offer adequate protection for their users.

Civil enforcement by the FTC is an important backstop to protect consumers against unfair or deceptive data security practices. In this testimony, I suggested three steps that Congress might take to empower the FTC in this mission: allowing civil penalties for first-time violators; authorizing data security rulemaking; and enabling the creation of a stronger technology workforce at the FTC.

I thank the Committee members for your attention to data security, and for the work that you have already done to protect the security of Americans' data; and I look forward to your questions.

The CHAIR. Thank you. And I knew there was something there—Dr. Felten—I thought it was Dr. Felten, and I should have known that because it is the University of Washington that you graduated from. So, thank you. Thank you for that. We will ask you more about the technology aspect of this, because I do think the work-

force is a very big issue. Ms. Tummarello, thank you so much for being here.

**STATEMENT OF KATE TUMMARELLO, EXECUTIVE DIRECTOR,
ENGINE**

Ms. TUMMARELLO. Thank you. Chair Cantwell, Ranking Member Wicker, members of the Committee, thank you for the opportunity to testify before you today. My name is Kate Tummarello, and I am the Executive Director of Engine, a nonprofit that works with a nationwide network of thousands of startups to advocate for pro-innovation, pro-entrepreneurship policies.

Most of the current technology policy debates focus on concerns about how the largest players handle or mishandle consumer data. But startups are critical contributors to innovation and economic and job growth in the U.S., and they have a unique perspective and need, a data security framework that accounts for the breadth and diversity of the startup ecosystem, sets clear consistent expectations, and protects responsible actors from unwarranted legal and compliance costs in worst case scenarios.

For many startups, data security is a business imperative. Startups often don't have the name recognition or long standing relationship with consumers that larger companies do. While high profile data breaches of large corporations take up headlines and Congressional attention, those companies live to see another day. For a startup, one data breach can drive away users and investors and ruin a company. Startups have to constantly balance competing goals while building out a successful product or service. One of the many things they have to consider is securing user data.

In fact, many startups see privacy and security as a competitive advantage and use strong security measures as a way to differentiate themselves from others in the industry. But every startup has to grapple with the fact that it could be the victim of a data breach, as there are at least a thousand every year and unintentional errors can still happen at responsible companies. The startup ecosystem isn't a monolith, and each company is risk assessment and security measures are going to look different.

A two person startup collecting non-sensitive data from a handful of users will have a very different risk profile than a larger company collecting sensitive data from thousands of users. At the same time, a new and small startup won't have the resources to spend on compliance and security measures that a larger company will. Being responsible stewards of user data will look different for every company, and Federal data security policy needs to recognize that.

As Aaron Vik, a startup advisor from Jackson, Mississippi told us, smart and helpful data security policy should promote flexible security practices, not make life harder for startups when they are victims of data breaches. And if a startup is a victim of a data breach, it has to spend its very limited time and resources detecting, mitigating, and investigating the breach, which can cost tens or even hundreds of thousands of dollars. By contrast, the average seed stage startup has about \$55,000 to spend per month, a sum that needs to cover salaries, equipment, research, development, marketing and more. And since the vast majority of startups do not

yet or do not yet—or do not yet have outside funding, many startups have significantly less than \$55,000 a month to spend.

A complicated regulatory and legal regime makes a disastrous situation for a startup worse in the wake of a data breach. Congress should create a Federal framework that gives startups clarity on the measures they need to implement to protect consumer data and clarity on the steps they need to take if they do suffer a data breach. A Federal framework should also create certainty that startups won't face regulatory and legal burdens if they do suffer a data breach despite their precautions. The current patchwork of State laws provides unclear data security standards on the front end and varying or even conflicting requirements in the wake of a breach, which creates ambiguity and uncertainty for startups.

For example, in notifying users of a breach, Michigan law requires companies to describe the incident that led to the breach, while Massachusetts prohibits notices containing that sort of information. And because startups almost always have users in multiple states, the first step of notifying users of a data breach can involve hunting down additional user data the company might not otherwise have or need to determine where users are located, and which State laws are implicated. In addition to having to navigate State laws, startups also have to worry about being sued in multiple states.

A lawsuit, especially one where an organization's data security measures are dissected in a lengthy discovery process, can easily cost hundreds of thousands of dollars in legal fees. This approach to enforcement also opens up the door for courts to issue inconsistent rulings about what security measures are adequate under the law. It also creates opportunities for malicious or misguided lawsuits, where, for instance, a startup is sued by a competitor or faces a nuisance value lawsuit. Again, a Federal framework should create clarity and consistency and restrict the opportunities for bad faith litigation.

One bright spot in the current policy landscape is where State laws incentivize security measures by, for instance, easing compliance burdens if a data breach impacts only encrypted data. Encryption is one of the most effective ways startups can secure their users' data. As Ben Golub, CEO of Atlanta-based Storj explained, the widespread use of encryption is key to protecting sensitive consumer, financial, health care, and research data from compromised by us or by bad actors, and these are the kinds of measures we should be encouraging.

Congress should create a Federal framework that incentivizes a strong security measure that makes sense for startups and their unique risk profiles, allows room for the universe of responsible security measures to grow and adapt as the threat landscape evolves, and creates consistency and certainty for responsible actors, including ensuring they won't face unnecessary burdens in the event of a data breach.

We appreciate the Committee's attention to this issue and the broader effort to create a Federal privacy framework. To quote Tony Hyk, CEO of Minneapolis-based TheraTech, "if lawmakers are going off an assumption that every business is trying to do bad things, then they don't understand startups. There will be a few

bad actors but legislating for the lowest common denominator is not the right approach.” Thank you for your time and I look forward to answering your questions.

[The prepared statement of Ms. Tummarello follows:]

PREPARED STATEMENT OF KATE TUMMARELLO, EXECUTIVE DIRECTOR, ENGINE

Chair Cantwell, Ranking Member Wicker, members of the committee, thank you for the opportunity to testify before you today. My name is Kate Tummarello, and I am the executive director of Engine. Engine is a non-profit organization based in Washington, D.C. that works with a nationwide network of thousands of startups to advocate for pro-startup, pro-innovation, pro-entrepreneurship policies.

I’m especially appreciative to be here today, because most of the current technology policy debates focus on concerns about how the largest industry players handle, or mishandle, consumer data. But startups are critical contributors to innovation and economic and job growth in the U.S. and have a unique perspective and need: a data security framework that accounts for the breadth and diversity of startup companies; sets clear, consistent expectations; and protects responsible actors from unwarranted legal and compliance costs in worst case scenarios.

For many startups, data security is a business imperative. Startups often don’t have the name recognition or long-standing relationship with consumers that larger companies do. While high profile data breaches of large corporations and major retailers may take up headlines and congressional attention, those companies live to see another day. For a startup, one data breach can drive away users and investors and ruin a company. Startups have to constantly balance competing goals while building out a successful product or service and cultivating a satisfied user base—one of the many things they have to consider is securing user data. In fact, many startups see privacy and security as a competitive advantage and use strong security measures as a way to differentiate themselves from others in the industry.

But making user trust and data security a priority doesn’t mean a startup, or any organization, can’t become the victim of a cyberattack. In fact, every startup has to grapple with the fact that it could be the victim of a data breach. According to the Identity Theft Resource Center, there have been more than 1,000 data breaches every year since 2016,¹ and data breaches in the first half of 2021 are on pace to exceed last year’s numbers.² We sometimes hear about obvious, irresponsible behavior—like losing an unencrypted hard drive—but unintentional errors can still happen at responsible companies. If one employee responds to a phishing e-mail or uses the same password across multiple services, a data breach can occur.

The startup ecosystem isn’t a monolith, and each company’s risk assessment and security measures are going to look different. A two-person startup collecting non-sensitive data from a handful of users will have a very different risk profile than a larger startup collecting sensitive data from thousands of users. At the same time, a new and small startup won’t have the resources to spend on the security and compliance measures that a larger company will. Being responsible stewards of user data will look different for every company, depending on its resources as well as the sensitivity and amount of data it has. Federal data security policy needs to recognize that. As Aaron Vick, a startup advisor and former startup CEO from Jackson, Mississippi put it, “smart data security practices will and should look different for every startup. Smart and helpful data security policy should promote flexible data security practices, not make life harder for startups who are victims of data breaches.”

And if a startup is a victim of a data breach, it has to spend its very limited time and resources detecting, mitigating, and investigating the breach. According to a recent survey, small firms suffer the largest losses from cyber threats relative to company size. Companies with fewer than ten employees reported spending a median of \$8,000 in response to cyber attacks, but for some those costs climbed higher than \$300,000 per year.³ By contrast, the average seed-stage startup only has about

¹2020 in Review: Data Breach Report, Identity Theft Research Center 10 (Jan. 28, 2021), <https://notified.idtheftcenter.org/s/2020-data-breach-report>.

²First Half of 2021 Data Breach Analysis, Identity Theft Research Center 1, 2, <https://notified.idtheftcenter.org/s/2021-first-half-data-breach-analysis> (last visited Oct. 4, 2021).

³Hiscox Cyber Readiness Report 2021, Hiscox 9 (Apr. 2021), <https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber%20Readiness%20Report%202021.pdf>.

\$55,000 to spend per month⁴—a sum that needs to cover salaries, equipment, research, development, marketing, and more. And since the vast majority of startups do not, or do not yet, have outside funding, most startups have significantly less than \$55,000 per month to spend.

A complicated regulatory and legal regime makes a disastrous situation worse for a startup in the wake of a data breach. Congress should create a Federal framework that gives startups clarity on the measures they need to implement to protect consumer data and the steps they need to take if they suffer a data breach. A Federal framework should also create certainty that startups won't face legal and regulatory burdens if they suffer a data breach despite their precautions.

The current patchwork of state laws provide unclear data security standards on the front end, and varying or even conflicting requirements in the wake of a breach, which creates ambiguity and uncertainty for startups that want to protect their users. For example, in notifying users of a breach, Michigan law requires companies to describe the incident that led to a data breach, while Massachusetts prohibits notices containing that sort of information.⁵ And because startups almost always have users in multiple states, the first step of notifying users of a data breach can often involve hunting down additional user data the company might not otherwise have or need to determine where users are located and which state laws are implicated. These state-by-state differences drive up startups' compliance costs without making consumers any safer.

In addition to having to navigate state laws, startups also have to worry about being sued if they are victims of a data breach in some states. A lawsuit—especially one where an organization's data security measures are dissected in a lengthy discovery process—can easily cost hundreds of thousands of dollars in legal fees,⁶ which would entirely deplete a startup's limited resources. This approach to enforcement also opens up the door for courts to issue inconsistent rulings about what security measures are adequate under the law,⁷ which creates compliance confusion and costs that fall disproportionately on startups. It also creates opportunities for malicious or misguided lawsuits where, for instance, a startup is sued by a competitor or faces a nuisance value lawsuit and chooses to settle rather than engage in lengthy and expensive litigation.⁸ Again, a Federal framework should create clarity and consistency and restrict the opportunities for bad faith litigation.

One bright spot in the current policy landscape is where state laws incentivize security measures by, for instance, easing compliance burdens if a data breach impacts only encrypted data. Encryption is one of the most effective ways startups can secure their users' data, and startups can benefit from policies that encourage and incentivize strong security measures, including encryption and data minimization. As Ben Golub, CEO of Atlanta-based encrypted, decentralized cloud storage company Stori, explained, “we design our decentralized systems so there are no single points of failure, and so that they are highly resistant to both traditional and ransomware attacks. The widespread use of encryption is key to protecting sensitive consumer, financial, healthcare, and research data from compromise—by us or by bad actors—and those are the kinds of measures we should be encouraging.”

As Congress considers ways to increase data security for consumers across the Internet, lawmakers should keep startups in mind. Congress should create a Federal framework that incentivizes strong security measures that make sense for startups and their unique risk profiles, allows room for the universe of responsible security measures to grow and adapt as the cybersecurity threat landscape evolves, and creates consistency and certainty for responsible actors, including ensuring that they won't face unnecessary burdens in the event of a data breach.

Finally, Congress should promote training and support for a top cybersecurity talent pool—and therefore a diverse cybersecurity talent pool—because these professionals will be vital to keep pace with emerging technology and new threats, and because they can (and should) be a part of ongoing policy discussions about data

⁴*The State of the Startup Ecosystem*, Engine 17 (Apr. 22, 2021), <https://engineis.square.space.com/s/The-State-of-the-Startup-Ecosystem.pdf>.

⁵Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. Ill. L. Rev. 811, 838–39 (2020).

⁶Marcia Ernst, *Data Breaches: They're Not Just Problems for the IT Department—They Can be Legal Headaches Too*, SGRLAW (Summer 2016), <https://www.sgrlaw.com/ttl-articles/data-breaches/>.

⁷*Cf.* Kosseff, *supra* note 5, at 823–27 (discussing the possibility of shifting or unclear decisions in data security orders).

⁸*Cf.* *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits*, U.S. Chamber Institute for Legal Reform (Aug. 31, 2017), <https://instituteforlegalreform.com/research/tcpa-litigation-sprawl-a-study-of-the-sources-and-targets-of-recent-tcpa-lawsuits/> (discussing expanding trends in Telephone Consumer Protection Act suits targeted against legitimate U.S. businesses, and not just “unscrupulous scam telemarketers”).

security. As Safi Mojidi, Founder of Hacking the Workforce, has explained: there are “legislative gaps [that] should be addressed immediately in order to achieve more consistent standards for how organizations use personal information, while also providing industry with clear national guidance on how to protect privacy and security. [But w]hen thinking through the consequences of policy decisions, we need to make sure we have some of the brightest, diverse minds in the room, who can think about the impact on entire communities that policies would have.”⁹

We appreciate the committee’s attention to this issue and the broader effort to create a Federal privacy framework. We hope lawmakers will continue to take into account the unique challenges startups face in this space and find a legislative solution that works for the thousands of startups that want to be secure, responsible, and successful. To quote Tony Hyk, CEO of Minneapolis-based digital health startup TheraTec, “if lawmakers are going off an assumption that every business is trying to do bad things, then they don’t understand startups. There will be a few bad actors, but legislating for the lowest common denominator is not the right approach.”

The CHAIR. Thank you. Thank you for all the testimony today. I want to do as we did our last hearing, try to figure out whether we have a lot of commonality. So if you could just kind of be brief on answers, if you could. Do you all support an FTC Privacy and Data Security Bureau?

Mr. LEE. Yes.

Ms. RICH. Yes.

Mr. FELTEN. Yes.

Ms. TUMMARELLO. Yes.

The CHAIR. Do you support first time penalties? If somebody knows the answer—

Ms. RICH. Yes.

Mr. LEE. Yes.

Ms. TUMMARELLO. Yes, if there are clear rules of the road.

Mr. FELTEN. Same.

The CHAIR. OK. Do you—on this technology issue, one of the key things, Dr. Felten, is to get technology workforce at the FTC who understands these issues. Ms. Tummarello is bringing up a point about small businesses, but I venture to guess knowing what I have known about the past cases at the FTC, is that the people who are the breach and privacy violators are those who don’t have the workforce within their organizations or understand their responsibility as it relates to data and the threat. I don’t know if Mr. Lee might see the same thing.

Juxtaposed to startups who are very sophisticated technology players because they wouldn’t be in that business if they weren’t very sophisticated technology players. So what we are seeing is an absence of technology expertise at these firms, is that correct? The ones that are getting the violations. And Ms. Rich, you can join in here too. Is that what we saw at the FTC?

Ms. RICH. I wouldn’t totally agree with that. Sometimes that was the case, but sometimes it was simply a failure to prioritize it or put the investment there. So—

The CHAIR. That is exactly my point—

Ms. RICH. Yes—

The CHAIR. Companies have a lot of data.

Ms. RICH. Yes—

The CHAIR. And then they don’t prioritize—

Ms. RICH. Right—exactly.

⁹ #StartupsEverywhere profile: Safi Mojidi, Founder, Hacking the Workforce, Engine (July 9, 2021), <https://www.engine.is/news/startupseverywhere-alexandria-va-hacking-the-workforce>.

The CHAIR. Which I consider somewhat being sophisticated—that level of data. So that is the point. So that is—who was violating the FTC’s actions against people were people who weren’t taking that responsibility seriously.

Ms. RICH. Exactly.

Mr. FELTEN. Yes. Often, it is a failure to take sufficient care, meaning not recruiting the technology people you need, not managing them carefully, not making this an issue that is on the radar of senior officials in the company. That is what leads to sloppiness and corner cutting, which ultimately is the cause of a lot of these problems.

The CHAIR. So, Mr. Lee, your report show that we had a hearing more than a year ago about Equifax and its breach, which was simply not applying a patch that was a known solution. But you are saying we are beyond that even. We are beyond the people just not doing patches, because now the attacks, because people understand the amount of money and resources here, are much more sophisticated.

Mr. LEE. We have gone from a period of data acquisition. So let’s think of Equifax as sort of the high point where bad guys wanted to accumulate as much data as they could from as many sources that they could find. Now we are into a period where they are using the data they have already stolen. So we have gone from a period of theft to a period of fraud.

So a lot of what you are seeing in the last year has been circumstances where they will use that to either perpetrate a phishing attack that can lead to ransomware, can lead to that kind of information when you have a log in and password from an organization that can lead directly into a ransomware attack because they can, they don’t need to breach your system, they can go in with a log in and password. Or you have what you saw with unemployment, where you can pretend to be individuals and open up accounts or take over accounts.

So we have gone from acquisition to fraud. Now that doesn’t mean they are not still trying to acquire, and they are not still using our own tools against us. We don’t patch fast enough. We have legacy software that hasn’t been updated or replaced in in some cases decades, but certainly you have a lot of legacy software out there in organizations. Time consuming—it is expensive, I understand that, but it still has to be done, and that leads to the attacks like what you saw at Accellion.

The CHAIR. And so, Dr. Felten, what do you need to require of the companies as it relates to the level of technical sophistication that they should have in dealing if they are, let’s just say, dealing with large volumes of public content.

Mr. FELTEN. Yes, the bar is certainly higher for them, needs to be higher for them than it has been because the threat is higher. It requires—it requires staff, it requires especially a sophisticated and strategic approach to managing these systems, and it requires consistent execution.

Companies need to be willing to in some cases spend money, in some cases encounter inconvenience to upgrade legacy systems and so on, in order to protect things because what the community has learned over and over is that a single failure to patch one thing or

to upgrade something when it needs to be there, to make sure that some digital door is locked can lead to a huge breach.

The CHAIR. Thank you. Senator Wicker.

Senator WICKER. Thank you, Madam Chair. Let's go down the line on some other questions. Do you all support inclusion of a data security requirement in a Federal data privacy law?

Mr. LEE. Yes.

Ms. RICH. If a—I wouldn't want to hold it up for what is turning out to be a very difficult process of negotiating a privacy law, which is very broad. So if you could enact a data security law on its own, it would substantially improve data protection in this country.

Mr. FELTEN. Yes.

Ms. TUMMARELLO. Yes.

Senator WICKER. OK. Agree or disagree with this statement. Let's start with Ms. Tummarello and go backward. A preemptive Federal law does not mean a weaker law.

Ms. TUMMARELLO. Agree.

Mr. FELTEN. Yes, it is not necessarily weaker.

Ms. RICH. If it is a strong law, it is not weaker.

Mr. LEE. Yes.

Senator WICKER. OK. And let me ask you, Ms. Rich. On your statement, your oral statement about a private right of action, is that consistent with your written statement or have you changed your position? I am just not sure we all heard you correctly there.

Ms. RICH. My position, I thought, was consistent between my statement—

Senator WICKER. OK, well just tell—tell us what it is.

Ms. RICH. Is that if it is a strong law, with strong penalties—with strong remedies, resources for the FTC, State AG enforcement, a private right of action is not necessary. However, if there—if it just continues to be this very difficult issue, there are middle grounds to consider. But I don't personally think it is necessary.

Senator WICKER. OK, good. Now, on page seven of Mr. Lee's testimony, he states, "in the environment where we operate today, some states are more aggressive in protecting their citizens and others, resulting in disparate impacts for the same crime based on where you live. Victims and businesses alike are well served when everyone knows the rules and face the same consequences." Mr. Lee, that is an argument for preemption, isn't it?

Mr. LEE. Not necessarily. What we believe is that victims need options. And we are—you know, we are here today advocating for victims and the redress that is available to them. But what we see today is, when every part of the process, whether it is the enforcement of whatever a State has deemed to be a data breach all the way to the form of the notice and the substance of the notice, we are so across the board in so many different areas, it is very difficult for anyone to have any kind of understanding if you are the business or you are the victim of what it is that I can do to protect myself or what is it that somebody is going to do to protect me.

Senator WICKER. OK. You may want to enlarge on that on the record. Ms. Rich, I think Mr. Lee's written statement makes a case for preemption. Do you agree?

Ms. RICH. You are trying to get us to argue?

[Laughter.]

Senator WICKER. I am trying to compare and contrast.

Ms. RICH. I think that the case for preemption, if the law is strong and all the State AGs enforce it, is very strong.

Senator WICKER. And that would prevent situations in which the same crime based on where you live has disparate impacts, would it not?

Ms. RICH. Yes.

Senator WICKER. Now, OK, Mr. Lee, I think Senator Cantwell and I, I think she will give us a little leeway here. I think we are interested in a ranking of who is doing a good job. Now, I think what I understand you to say is you think there are just as many breaches in the United States as there are in the EU. They are just not being reported, and the difference is grossly—I mean, it is just obvious. Is that correct? And also where—which data security laws are doing a really, really good job? And how can you prove that?

Mr. LEE. Great question.

Senator WICKER. I just think Senator Cantwell wanted me to ask that.

Mr. LEE. Well, also to answer to both of you then, we do believe that it is obvious. We know because of the disparate nature of State regulations and State laws. What is a breach in one state is not a breach in another state? That in and of itself tells us that we are not being—we are not having uniform reporting. I can give you two examples of large breaches that impact—has impacted millions of people, but there is never been a single data breach because the organization deemed it doesn't apply to us.

Now that is being litigated. We are going to find out if it applies to them. But their position is we had a breach, we were attacked, we had a ransomware attack, but we are not responsible for notifying any victims because we were just holding the data of our customers.

Senator WICKER. Must that be reported in one state and not another, and must that be reported in the European Union and not in half the states?

Mr. LEE. That would be correct. There are states that do not require that.

Senator WICKER. Which State has the best law in your judgment?

Mr. LEE. Actually, Maine has a tremendous data breach law and a tremendous data breach reporting system. We get some of our very best data from the State of Maine. There are a number of States that have very good laws. Obviously, you know, California with the genesis of data breach laws being in California, they have a very strong law. New York has a very strong law. New York has very strong regulations underneath that.

Senator WICKER. And there are results to prove this?

Mr. LEE. Yes, sir.

Ms. RICH. Can I make just a quick comment? I think what is missing is data security. Data breach is great. Data breach notification laws are great. They create accountability, but they put the burden back on consumers to protect themselves. And what I thought we were talking more about here was having a data security standard to prevent breaches in the first place. And that is critical.

The CHAIR. Senator Baldwin is next. Thank you.

**STATEMENT OF HON. TAMMY BALDWIN,
U.S. SENATOR FROM WISCONSIN**

Senator BALDWIN. Thank you, Madam Chair. I want to focus a little bit on the security issues that Chair Cantwell brought up that resulted in the big breaches. So things as simple as failure to install a software patch or failure to encrypt user information.

We know the Equifax breach was possible because the company failed to apply a patch and the Colonial Pipeline ransomware attackers infiltrated a virtual private network account that didn't use multifactor authentication—authentication, which is a basic cybersecurity tool. Dr. Felten, in light of that reality, how should we be thinking about best incentivizing companies to do what should frankly be common sense cybersecurity practices?

Mr. FELTEN. Well, I think there is—there is by now a well-established list of basic practices, including the ones you mentioned, and I suggest a longer list in my written testimony. But in my view, a rulemaking might require companies to follow those basic practices, in addition to the process and accountability, internal control considerations that will help to protect against more sophisticated attackers and more subtle errors. This is—these baseline practices, I think, ought to be required.

Senator BALDWIN. Ms. Tummarello, you talked in your testimony about the fact that small businesses don't have the same resources to ensure compliance with data security requirements. And frankly, if we don't expect a major company like Colonial Pipeline to take the basic steps on data security, do you think it is unfair to expect a company with perhaps only a few staff or no in-house IT expertise to succeed where large and well-resourced companies have failed?

That is rhetorical. Let me just ask specifically, how do you think Congress can ensure that smaller businesses engage in appropriate data security practices? And how should small business—the carrots and sticks for small businesses be different than those of large businesses that are well resourced?

Ms. TUMMARELLO. Thank you for the question, Senator. I think, you know, first and foremost, the vast majority of startups want to do the right thing, and currently they are stuck trying to figure out what exactly the right thing is. And so clear, consistent guidelines, whether through an FTC rulemaking or elsewhere, just saying here is the menu of options that count as responsible security practices, and if you do these, we know that we can't prevent 100 percent of cyber-attacks, but this is what responsible behavior looks like and this is what you should model after, I think that would be a huge step up for startups that want to do the right thing, but again, just don't know what it is.

And I would hope that any kind of menu of options provided by, for instance, in FTC rulemaking would account for scale and size and resources. Some of the things you mentioned in your first question are low hanging fruit, and a startup can easily do them. It is just needing to know that that is enough. And so I think there is a way to create a framework that allows flexibility but still provide startups the certainty they need.

Senator BALDWIN. Yes. Well, speaking of resources, I think there is agreement that the Federal Trade Commission does not have sufficient resources and staff today to handle the issues related to data security and data breaches. I wonder if you can, Dr. Felten and Ms. Rich, talk about what kind of additional needs the agency has if Congress were to expand its authority on data security.

Mr. FELTEN. So in terms of staffing of technologists, I think the agency is on the order of 10 professional technologists who are working in the mission side of the agency right now. And I think with resources, the FTC could reasonably use 50 to 60 people in those roles.

Ms. RICH. In addition to—to help attract technologists, there have actually been a few serious problems that have been identified by former technologists at the agency other than Ed. One is there is no career path, as Ed talked about, but another is that there are very rigid and outdated ethics rules governing what technologists can do when they leave the FTC.

That ends up meaning that if they ever worked on a case involving Google, they can never work on any other case involving Google. So it is a big disincentive in some articles have been written about it. In terms of what the FTC needs, it is not just money, it is authority. I worked for years with Section 5, trying to bring privacy and data security cases, and they are really tough because there is so many gaps.

Section 5 doesn't even allow you to prescribe practices, it only allows you to get an order against a company that already engaged in negligent practices. And it doesn't cover certain entities, and we talked about the civil penalties, et cetera. So there just needs to be a law that allows the FTC to hang its hat on it and hold companies accountable.

Mr. FELTEN. And I agree with the point about overly rigid conflict of interest rules.

Senator BALDWIN. Thank you.

The CHAIR. Thank you. Senator Blunt.

**STATEMENT OF HON. ROY BLUNT,
U.S. SENATOR FROM MISSOURI**

Senator BLUNT. Thank you, Chairman. Ms. Rich, I want to get to another topic here, you mentioned in your testimony that examples of data were account credentials, health data not covered by HIPAA, and precise geolocation data. Senator Schatz and I, both on this committee worked in the last Congress to try to get more attention to facial recognition standards.

I wonder if you would talk about that, and then if anybody else has an opinion on the use of this data and how there—and the lack of standards for collecting that kind of data that is out there, everything from whether you are on a screen and looking at something and you are recognized facially, or you are walking through a drugstore. There is all kinds of this out there and wondering what you are thinking about it as one of the things we should be concerned about.

Ms. RICH. Absolutely. I didn't happen to mention biometric data in my testimony, but it is absolutely part of the class of sensitive data that should be protected by any data security law. It also has

a lot of privacy issues associated with it. And right now, other than the FTC Act and the extent to which it falls, for example, under HIPPA, which still only covers a segment of hell of health data, there is really no Federal law that mandates security for biometric data.

Senator BLUNT. Alright. Mr. Felten.

Mr. FELTEN. Facial recognition particularly is an area that poses a lot of risks for consumers, because of the way that facial images can be captured at a distance and used without consent or even awareness of the consumer. So I think it is an area that requires special attention, even relative to the already serious other security issues.

Senator BLUNT. Mr. Lee.

Mr. LEE. Certainly made great points about the issues of capture. From our perspective is if your biometric is somehow compromised, you can't change your biometric. You can't change your fingerprint, you can't change your face, your retina scan, your voice print. So we need to be very careful about how we protect that kind of data, and we have to have very specific ways of helping people who are—whose identities are compromised when that biometric data is indeed compromised. And we don't really have a good framework for that today.

Senator BLUNT. Ms. Tummarello.

Ms. TUMMARELLO. Thank you. I think definitely biometric data, including facial recognition data, should be considered sensitive and should face heightened privacy and security requirements. I do think we would want to be careful not to completely eliminate the opportunities to use it in innocuous and innovative ways, but totally recognize there is a bigger threat here and it makes sense to put extra precautions around it.

Senator BLUNT. Well, you know, one thing people don't want is walking through a grocery store and then suddenly start getting ads for products, so you get a little of that by looking up anything while you are in the grocery store from the geolocation side of this, but also from whether it is a grocery store or whatever else. While I have got Ms. Rich and Mr. Felten here, to the FTC, you are both really well grounded there, is trying to move toward more open hearings. Your view of whether that is—the challenges there and whether that is a good idea or not.

Ms. RICH. I don't believe the FTC is sharing nonpublic information in those open hearings, so I see nothing wrong with it. There have been—there has been some controversy about whether all the information that is needed has been circulated prior to the open meetings, but I think being more open is a perfectly legitimate thing to do.

Senator BLUNT. Mr. Felten.

Mr. FELTEN. Ensuring that nonpublic information is not shared at those hearings, if we assume that, then I think this is a good idea, the transparency about what it is that the Commissioners are concerned about, and openness to the public is really useful in a lot of different areas. So I think for the Commission to do an appropriate part of its work in public is a positive step.

Senator BLUNT. There seem to be some early transition questions about how to give notice and how much notice would be necessary

and if notice itself sort of takes away from looking at what the Commission is really talking about. But I may want to follow up with the both of you. Is there any—I don't know—I think this is pretty much an FTC question. Thank you, Chairman.

The CHAIR. Thank you. Thank you. Senator Tester.

**STATEMENT OF HON. JON TESTER,
U.S. SENATOR FROM MONTANA**

Senator TESTER. Thank you, Madam Chair. I want to thank you for having this hearing, and I want to thank the folks who have testified today. I appreciate your testimony and your expertise. I really don't know where to start, so we will start here. Let's start with you, Mr. Lee. When we are talking about data breaches and the potential for identity theft, has anybody done any work to find out how much of this identity theft information is coming from the private sector and how much is coming from Government agencies?

Mr. LEE. We actually tracked the source of information. Based on the publicly noticed data breach reports—

Senator TESTER. Yes.

Mr. LEE. So we can tell you, you know—

Senator TESTER. Can you give me any sort of statistics on data breaches and how often—I am talking about, I don't know, severe is in the eyes of the beholder, but how many are happening in Government versus business?

Mr. LEE. So let's just look at this, this quarter, which was completed last week. There were 446 data breaches. 21 of those were from Government agencies.

Senator TESTER. OK. And so we are basically talking in today's hearing, though I assume on the private sector businesses, correct?

Mr. LEE. Although they are all important.

Senator TESTER. But we are talking about empowering the FTC. And I wouldn't think the FTC has power over the Veterans Administration, but who knows. I want to clarify some things up. But it is not to get you and Ms. Rich to fight, but you had said that some of the states that had strong laws are Maine, California, and New York. Is that from a notification standpoint or is that from a data security standards standpoint?

Mr. LEE. It is actually from both. And one of the things that you are seeing at the State level is this convergence of what historically has been three silos. We have had privacy laws is one silo. We have had identity management as one. And then we have had, you know, cybersecurity. And there was very little cross-pollination. But now what we are seeing is that as states are beginning to adopt stronger laws, there are actually cybersecurity, privacy, and identity elements in all of those laws.

Senator TESTER. Yes. So this may be an unfair question because once again the viability of the law is in the eye of the beholder, but would you say that half the states have adequate security laws or three quarters, 30 out of 50? However, you want to do it.

Mr. LEE. Well, you know, every law is helpful, but there are—we have gone through a period of transition where a lot of the states have sort of caught up to more common kind of data. A lot of the states, only about half, don't recognize biometric data.

Senator TESTER. Would you agree, and not to get you to fight, but would you agree with that, Ms. Rich?

Ms. RICH. According to the State legislative website, half—half of the states have data security laws—.

Senator TESTER. Oh, and half have none at all?

Ms. RICH. All of the states have data breach notification laws. Yes.

Senator TESTER. OK. Alright. And I might be able to get to that if time goes on. This is a question for Kate Tummarello. Sorry, if I bust your name. But there was an answer to one of the questions that said, what the FTC needs is the authority to prescribe practices. Doesn't matter what I believe, or actually it does if we pass a law, but as a representative of the startups, how do you feel about that?

Ms. TUMMARELLO. I think the FTC could be empowered to set out, you know, a menu of options, right. Not every cybersecurity and data security practice is going to make sense for each company. But there are things that everyone should be doing, and there are certainly things that lots of folks that handle sensitive data should be doing or folks that handle a lot of data should be doing. And so having a flexible framework that allows companies to pick and choose the things that makes sense for their companies—

Senator TESTER. OK. So let me give you an example. And I don't know—I think the name of the company was D-Link, professor, isn't that correct? I don't know if they are a startup, I don't know if they have been around a long time, but it would seem to me the FTC should say, clean up your act or we are going to fine you till you don't exist anymore. How do you feel about that?

Ms. TUMMARELLO. Yes, I think the D-Link example is a great example of not just sensitive data, but kind of sensitive technical capabilities baked in. And it would make sense for the FTC to have especially prescriptive ideas there.

Senator TESTER. So they could be very prescriptive, is what you are saying.

Ms. TUMMARELLO. For a company handling sensitive data and sensitive technical capabilities.

Senator TESTER. OK. Alright. So this is just for my curiosity, Ms. Rich. And by the way, we are not picking on anybody. I appreciate all your testimony very, very much. But could you give me the definition of non-sensitive data versus sensitive data? And if not, we will turn to the professor.

Ms. RICH. I think that people regard simple name and address these days, since it's out in the public domain, as fairly non-sensitive.

Senator TESTER. So, let me ask you this. I am a farmer in my real life, and I drive down the road and there is an implement behind me that has a computer on it is collecting everything that I do, how much seed I put in the ground. I don't use fertilizer, but if they use fertilizer, they can do that. They can—I mean, all sorts of data. And some people don't think that that is sensitive data. Do you think that is sensitive data?

Ms. RICH. I actually don't think the distinction is that relevant, because if you have a scalable—a scalable data security program,

you are going to provide security for all your data. You just may provide more security for data that——

Senator TESTER. I understand that. But the question becomes for me, as the beauty is in that the beholder, I think that that data is sensitive and I don't want anybody else to have it, even though my name isn't attached to it. I don't want people to have it because the way computers work this day, they can figure out who is doing it. And so——

Ms. RICH. I think the issue is that companies have limited amount of money or many companies, especially the one Kate represents, and you should be taking care of all your data and trying to make sure it isn't breached. But when you have—when it is something—when a system is going to cost a lot of extra money to protect something in a really, really secure way, you want to make sure it is the really sensitive——

Senator TESTER. The good stuff——.

Ms. RICH. Kids or health, or—yes.

Senator TESTER. I am sorry, I ran over, Madam Chair.

The CHAIR. Thank you. Senator Fischer, and then Senator Klobuchar. Senator Fischer, are you available?

**STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA**

Senator FISCHER. Thank you, Senator Cantwell. And thank you to our witnesses for being here today. So much of our daily lives and work shifted on the online space during the COVID 19 pandemic. And this shift online also led to a spike in ransomware attacks and targeted our work patterns, how they were changing. I am sure many members of this panel know the local companies and organizations in their states that have been impacted by ransomware.

Just a couple of days ago, a company based in Lincoln, Nebraska, that hosts several online auctions for farm equipment, livestock, and land was hit by ransomware attack, and the company had to take all of its sites offline. It has been very concerning for me to see the rise in these attacks, especially in the Ag industry, which drives Nebraska's economy and makes up one-fifth of our Nation's economy. But no sector has been immune from these attacks.

Ms. Tummarello, how do we ensure any Government led solutions are responsive to cybersecurity across industries, particularly with the increase in ransomware attacks?

Ms. TUMMARELLO. Thank you for the question, Senator. Like I said, I think giving the FTC authority to issue a menu of options where a company can recognize, OK, I am in this sector, I handle this kind of data, these are my resources, here is what makes sense, would allow a model that scales not just across the tech sector, but to your point, across all sectors. Because at this point, data security problems aren't just in the tech sector. Every business online or offline has data and making sure there is a solution that works for them will ensure that we protect consumers not just in one part of the economy, but in the entire economy.

Senator FISCHER. Thank you. Mr. Felten, how do you believe that cybersecurity policy should address critical sectors such as agriculture and communications or energy?

Mr. FELTEN. Well, it is certainly true, as you said, Senator, that there is no sector that is immune from these issues, immune from ransomware or other sort of data security considerations. And one thing that I think is important to do is to make sure that the services and products that companies in these sectors use when they outsource some of their functions are providing the protection that they ought to be providing.

So ensuring that the division of responsibilities between a supplier and a company that is using a product or service are clear, so that responsibility for these problems doesn't fall between the cracks, is very important. And that is one thing that legislation or a regulation could help to clarify.

Senator FISCHER. Thank you. As we saw with Equifax's neglected patching policy, ensuring timely updates and patches is important for guarding against cyber vulnerabilities, but keeping software up to date isn't a simple cure all to ward off breaches. The SolarWinds cyberattack showed us all too clearly that software updates themselves could be compromised. Ms. Rich, as we look to create a solid basis for policy around data security and accountability, how do we also work toward the need to create more trust throughout the software supply chains?

Ms. RICH. As Professor—Dr. Felten just talked about, there really does need to be accountability through the supply chain, which really doesn't exist right now. So when you share data, you need to make sure you are sharing it with people who can handle it responsibly. You need to make sure you are not giving them data that is subject to controls without passing along those controls.

So that cascading set of responsibility is very important. I want to also mention, though, that we have talked a lot about—Kate has talked about a menu of options that the FTC could create. It is very important that whatever we, whatever you do—pass here is enforceable.

So that is why, in my testimony, I talk about process based requirements that are enforceable, coupled with more detailed guidance that is nimble that the FTC could issue on an annual basis that responds to, you know, up to date protections and technologies that gives that menu. But there needs to be an enforceable law or rule underlying it.

Senator FISCHER. OK. Thank you very much. Thank you, Madam Chair.

The CHAIR. Thank you. Senator Klobuchar.

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

Senator KLOBUCHAR. Thank you very much, Madam Chair, for not only today's hearing, but the Subcommittee and Full Committee hearing yesterday. We are on the move in Commerce, and we are on the cutting edge as all of you are in discussing the issues of our day, which is what do we do about data?

What do we do about privacy rules? And as I argued yesterday, we simply cannot, and I appreciate Senator Cantwell's leadership in the privacy area, we cannot have this gigantic change in our economy like anything we have ever seen in the last few decades, some of it good, some of it bad, some incredible innovations, you

know, like the Fitbit I am wearing right now. But also, as we know, one of the jobs of Government, number one job is to keep people safe.

And as we heard yesterday, that is not always happening as we hear from these cyber-attacks. So we need to make our laws as sophisticated as the companies in our economy. And that means upgrading our laws and updating them. And so I appreciate you being here today. I think we need a national privacy law that creates digital rules of the road, and we need the resources for our agencies to enforce them. They are two separate things, but you can't have one without the other.

And I joined Senator Cantwell, and Schatz, and Markey in introducing a comprehensive privacy legislation to ensure that consumers can access and control how their personal data is being used. Do you all agree that consumers should have the ability to control their own data? Is that an agreement, all of you?

Mr. LEE. Yes.

Senator KLOBUCHAR. OK. Everyone else?

Ms. RICH. I think a privacy law should go further than consumer control, which is notice and choice, which we have seen is problematic. It should provide more substantive protections as well.

Senator KLOBUCHAR. Thank you. I think one of the things that was interesting was recently when Apple gave their customers a choice about protecting their data or not. And what was it? You can maybe explain better for me here, but 75 percent of their customers, is the number out there, chose not to have their data used. And it just shows us what would happen if this was available with all platforms. Professor Felten, in your testimony, you note that we can empower the FTC by authorizing data security rulemaking. Why is this rulemaking so important to protect consumers' data?

Mr. FELTEN. For a couple of reasons. First, that it provides more specificity than is available through the current structure of the FTC Act, so that companies have a clear idea of what they are expected to do. And it can also help to clarify ideas such as—clarify issues such as the responsibility of suppliers in a supply chain. So that there is not ambiguity about what companies are expected to do, and therefore there can be strong enforcement if they fail to do it.

Senator KLOBUCHAR. Thank you. And Ms. Rich, the bill would also increase transparency and require companies to maintain certain standards for their data security. In your testimony, you note that it can be a problem in companies over collect or over store data. How could a Federal privacy law help with this issue?

Ms. RICH. I believe that both bills, they are a little different, but they both talk about data minimization and reducing unnecessary collection and storage of data, and that would be a very important component of a data security law.

Senator KLOBUCHAR. And are you aware that one of the proposals out there as we debate this build back better agenda and making our laws sophisticated and putting people first, some of it is putting some funding into the FTC for privacy, as well as for my position as Chair of the Antitrust subcommittee, we hope additional resources on antitrust at both the FTC and the Department

of Justice. Could you talk about how important that is to have those resources?

Yes, the privacy bureau. I know Senator Cantwell asked all of you that question, but also the resources for these agencies to do their jobs.

Ms. RICH. The FTC's resources in privacy and also antitrust, but I am less familiar with that, is miniscule compared to other comparable enforcers abroad or even sectoral enforcers here in the United States. 45 to 50 attorneys, that was the maximum when I was there working on privacy. So resources are a critical piece of this as well as authority.

Senator KLOBUCHAR. I keep reminding people these are the biggest companies the world has ever known. Several of them are over trillion dollars, and we are trying to fight this with duct tape and Band-Aids. The other thing I like to remind people is in the competition policy area. And when we add resources to that, and I am sure the same could be said of some of the privacy work, we actually bring in money for the Government because they are doing their jobs and they are enforcing the laws. And so we are literally, as, you note Ms. Rich, these agencies are a shadow of their former selves, even during Ronald Reagan.

And that is why we have long neglected them. And there are, in the compensatory deals that Bill Baer, the former head of antitrust under President Obama, said shouldn't be getting out of the boardroom. And I can think the same could be said of policies that are hurting people's privacy. Because if we are not there on the other side, you know, creating that safety for people and making clear we are going to be tough and strong, then they are just going to push the max, as we saw yesterday from the whistleblower.

They are just going to target kids with bad anorexia content and the like, or let the algorithms do that and not do anything about it. That is what is going to keep happening unless we strengthen our side of the table. So thank you very much for your work, and I have some questions on cyber threats and the like which I will be putting on the record. Thank you.

The CHAIR. Senator Cruz, are you ready? Senator Cruz.

**STATEMENT OF HON. TED CRUZ,
U.S. SENATOR FROM TEXAS**

Senator CRUZ. Thank you, Madam Chairman. Welcome to each of the witnesses. There seems to be pretty broad agreement across the witnesses today that the way we currently handle the issue of data security at the Federal level is at best a patchwork, and a problem made worse by a patchwork of different State laws across the country. At the Federal level, there is a multitude of rules, regulations, guidances, not to mention outdated statutes, some of which were enacted at a time when cars were brand new technology. And together, that creates confusion and uncertainty among companies and consumers, and often leaves regulators powerless to address genuine harm. And leaves the American public significantly vulnerable. I want to start with a simple question to all the witnesses, let's say Congress can somehow get to yes on a sensible data security law. Who should be responsible for it? The FTC, somebody else?

Ms. RICH. The FTC has the experience and the expertise in this area and the will to protect consumers in this area. It has been trying to do that for 20 years. It is absolutely the right agency, but with the resources it needs and the authority it needs.

Senator CRUZ. Any disagreement on that question?

Mr. LEE. No, the FTC has had a mission of consumer protection for its whole history. It is the right agency for this.

Senator CRUZ. So if the FTC has the principal authority, should the FTC also have the authority to harmonize regulations and guidance across Federal agencies? So for example, should the FTC be able to tell the TSA that its cybersecurity regulations need to change one way or another? Tell HHS that it needs to beef up minimum standards for what is or isn't HIPPA compliant?

Ms. RICH. I think that is putting the FTC in a very difficult position, and I would not recommend that. I would say that you should do that. You as a body should decide how the regulations and laws harmonize.

Senator CRUZ. Anyone have a different perspective? So there should be no regulatory role for harmonizing regulations?

Ms. RICH. No, there certainly should be discussions about harmonizing it, I just don't think the little FTC should be the one telling all the other agencies what to do. They are equal players and that is something maybe OMB could do, or Congress could do.

Senator CRUZ. Let's focus then on how Congress and or the FTC strikes the right standard, strikes the right standard that has the substance needed to be effective, while also the flexibility to be applicable to companies with very different risk profiles. What do the witnesses think the guidance should be on that?

Ms. TUMMARELLO. Thank you for the question, Senator. I think the FTC could issue kind of a menu of options where startups and bigger companies and other organizations can decide what makes the most sense for them, knowing that they are meeting some kind of minimum standard set by the FTC, so that if something does go wrong, because again, not all data breaches can be prevented, they have done the right thing. And again, startups just want to do the right thing and would appreciate guidance on what that right thing is.

Mr. FELTEN. I think there are some baseline practices that companies across the board ought to be following, and some of those are listed in my written testimony. But beyond that, I think it would depend, or it ought to depend on the amount and sensitivity of consumer data that a particular company is dealing with. So companies with more, and more sensitive data, could be held to a more stringent standard.

Ms. RICH. And in my testimony, I proposed that there be a process based law that is scalable, similar to the safeguards rule, the original safeguards rule, but maybe a little more meat on the bones of it. And then the FTC would provide Congressionally mandated annual updated guidance with that menu of option that Ms. Tummarello is discussing.

Senator CRUZ. And what are the risks of overregulation, of standards that are too strict and what are the potential downsides that could come from that?

Ms. RICH. They quickly become outdated as technology changes, and there is no chance for Congress to amend the law or rule-making to keep pace, or they are not suited for small businesses because they are too prescriptive in terms of technologies that may not be necessary for certain small businesses.

Senator CRUZ. So how do we avoid that risk?

Ms. RICH. I think by having a process based rule that is scalable based on the size of—the volume of information a company collects, the sensitivity of data, the nature of the operations, coupled with updated guidance that the FTC could issue on an annual basis or more. Thank you.

The CHAIR. Thank you. Senator Hickenlooper.

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

Senator HICKENLOOPER. Great. Thank you, Madam Chair, and thank all of you for your time. This is something that I have—having been a Governor in Colorado, I am not ignorant of. I will start out with Ms. Tummarello. We signed into law a Colorado statute that requires reporting of security breaches of over 500 or more Colorado residents. Has to go to the Attorney General within 30 days.

We also created the National Cyber Security Center, which was and continues to be an effort to promote data security with both private and public companies with the NCC. We launched Cyber Security for State leaders, which is a Google effort to educate, provide a training curriculum for State officials, including county Commissioners and municipal folks.

Obviously, timely reporting, as you guys have all said, pays a lot of different dividends. How should we think about a national reporting process? I think everyone is kind of talked about the need for it. What would you say it should look like in terms of how do we—as a small businessperson for many years myself, I want to start with your perspective on that?

Ms. TUMMARELLO. Thanks for the question, Senator. I think first and foremost, one standard is a huge advantage for small businesses and startups. And we have talked a lot about data minimization at this hearing. And I think one of the points that gets glossed over is that if you are having to follow a State by State patchwork, you are having to collect information about where your users are located to figure out if those State laws are implicated.

And so creating a single standard not only incentivizes better data practices at the outset by not requiring State information, it also just makes it easier. If a startup is the victim of a data breach, it has to jump into action without having to figure out 50 State laws. And so I think you know it almost—a 30 day reporting requirement seems reasonable. It is more just about having one requirement across the board.

Senator HICKENLOOPER. Alright. I wasn't going to suggest that Colorado's be the model. But since you put it out there, Dr. Felten, I wanted to ask you a little bit about some of these ransomware attacks that we have seen so much of. We had a—in May 2020, JBS is a large meatpacker in Colorado, had a serious breach. We had a Colorado hospital that lost 5 years of electronic health

records from 2012 to 2017, and it took 6 months to recover a lot of the critical health data.

We have really pushed that businesses should provide security training for their employees, that they should have an incident response plan, that there should be a backup for their server data. So obviously, as you all know, that it is not a question of if, it is a question of when an organization or an enterprise is going to be breached.

So what—in your opinion, Dr. Felten, what targeted resources can Congress provide to support businesses' data security? In other words, what can we provide?

Mr. FELTEN. To support businesses specifically, I think there are important educational roles that Government can play. The FTC has an office that is engaged in this education for consumers and small businesses to help them understand what is out there and how to make safe decisions, giving them simple checklists of best practices and so on.

It becomes more difficult when you are talking about larger organizations that face more sophisticated threats. There, I think Government can help to play a convening role so that information can flow between organizations about what are the best practices and how can they protect themselves.

Senator HICKENLOOPER. Right. Well, I would probably go further than that, but I appreciate that. Mr. Lee. I was struck that in large part, what we are talking about here is security, the most basic type, and that the traditional way that we look at security in this country has been, you know, we have the Federal Government does national security and then most of us in our local communities have our local police department, is where we really look at security.

And yet right now, in terms of cybersecurity, it is largely relegated to the private sector and for individual small companies, large companies, health care providers, it is catch as catch can. How do you see that balance between private companies providing cybersecurity protection, and clearly what I think is becoming apparent, the public need?

Mr. LEE. It is a great question, Senator, and I was also struck by something you just said about the question of it is not a matter of if, it is a matter of when. It is actually a matter of how many times—

[Laughter.]

Senator HICKENLOOPER. Don't say that.

Mr. LEE. Unfortunately. The practical reality is, the private sector and the Government for their agencies are in the only position to be able to provide security and to prevent the kinds of incidents we are seeing that impact people, so create victims. So we have to have a partnership between all of the parties, beginning with Government setting a standard, an enforceable standard, that then the private sector can go and implement.

And they have the clear rules of the road. They know the consequences if they breach them, and they have the tools necessary to be able to implement them. If we have that system, we will reduce the number of cyber incidents, we will reduce the number of

data breaches, and we will therefore reduce the number of identity crime victims.

Senator HICKENLOOPER. I think that is something we can all work toward.

The CHAIR. Thank you.

Senator HICKENLOOPER. Thank you, Madam Chair,

The CHAIR. Thank you for that questioning. I am going to ask Senator Moran's indulgence. From the hearing the other day we had—there is some confusion, I am going to talk to Senator Wicker. And we had Commerce committee rules pre-COVID and then COVID adoption, and now we are still in a kind of a hybrid thing where some people are logging in, you know, remotely, so I think we have to figure out how to get back to what rules that we are going to operate under—.

Senator BLACKBURN. Exactly. And some of us logged in at the start of that hearing to get—.

The CHAIR. Well, I think—we will have—but I have asked Senator Moran for his indulgence today, given that we—.

Senator MORAN. I am very indulgent.

The CHAIR. So we really appreciate his—.

Senator MORAN. Madam Chairman.

The CHAIR. Yes, thank you.

[Laughter.]

The CHAIR. So Senator Blackburn, then followed by Senator Blumenthal. Then Senator Moran.

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

Senator BLACKBURN. Thank you so much, Madam Chairman. And to each of you, thank you. This has been such an interesting week. Yesterday we did privacy, kids' privacy in the online space, and of course, with data security today. But what I want to do is break out social media from small business and other interests.

And let's talk specifically, and professor, I am going to come to you on this first. Is there a—we know how social media is collecting data. They keep that data. They mine that data. Then they turn around, they sell the information in that data. So should there be a special set of obligations and enforcement and penalties that we expect from those social media companies?

Mr. FELTEN. In my view, social media companies differ from many other companies more in degree than in type when it comes to privacy. These are companies—these are among the companies to collect the most data that use it most aggressively. And so the need for strong rules of the road and enforcement would be strongest for those companies.

Senator BLACKBURN. So you would do a broader bill that would capture all entities. Would that be your approach?

Mr. FELTEN. I think a comprehensive data security framework is important, one that covers everyone, but that scales according to the volume and sensitivity of information that a particular entity has.

Senator BLACKBURN. OK. Ms. Rich, I see you are thinking out loud there with us.

Ms. RICH. Well, I am nodding, and I am shivering, too. It is really cold in here. But I agree with everything Professor Felten just said.

Senator BLACKBURN. OK. Thank you. So one set of rules, the entire Internet ecosystem. One regulator, the FTC. Platforms can't boot you off. That is basically where you all are.

Ms. RICH. This is one reason the FTC needs a lot more resources, it is because when they investigate a giant company like that, that is collecting a lot of data, that investigation is going to be really, really complex and take a lot of resources. But I do think it is important in this law, especially if it is going to have preemption, for the State AGs to also be able to enforce it.

Senator BLACKBURN. OK. Alright, Ms. Tummarello, the IRS data security breach.

That supposedly has the data on tax returns of thousands of people and may go back as much as 15 years into a person—this is something that is of tremendous concern. We know that as of last month, the IRS is still looking at this alleged breach, but now we are hearing that the Administration is wanting to propose a sharing of the information, letting the IRS look at every transaction, \$600 and above, and that amount of data and invasiveness is—that really carries a lot of privacy concerns for me. Tennesseans don't want that.

And they have really been quite vocal about this. But talk about the potential issues that you see with that type of invasive practice from an agency that has seen data security issues.

Ms. TUMMARELLO. Yes, absolutely. Thank you for the question, Senator. So we have thought about it, you know, because we are focused on startups in the cryptocurrency context, because there are cryptocurrency startups who don't want data, they don't want to have the data, they don't—they want to, you know, protect the privacy and security of their users. And we are always concerned about Federal rules that not only right might make it so that agencies can get the data, but that require companies to keep and get the data in the first place.

We have talked about data minimization. I think that is a great principle and one that should be baked into any privacy or security law. But anything that kind of counteracts that by requiring collection and storage of data in the private sector goes, you know, right up against what companies should be encouraged to do.

Senator BLACKBURN. OK. Madam Chairman, I am going to stop at that. I yield my time back. Thank you very much.

The CHAIR. Thank you. Senator Blumenthal.

**STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT**

Senator BLUMENTHAL. Thank you, Madam Chair. And thanks for having this hearing and for your work on data security. I am going to take advantage of this panel's very impressive expertise to talk a little bit about a topic we discussed yesterday in this room with Frances Haugen, the whistleblower in the Facebook documents, she spoke very powerfully and compellingly about the role that algorithms play in pushing harmful content on children. And obviously, the algorithms use data, so it is not completely unrelated.

She is a data scientist and engineer with an MBA from Harvard, and she spent years working on algorithms. And her observation was that the Facebook algorithm is a kind of black box. That is my word, not hers, because nobody outside Facebook knows how it works. And we conducted an experiment, my office did, creating a 13 year old girl on Instagram who expressed interest in weight loss and dieting and eating disorders, and she was flooded within 24 hours with accounts relating, or recommendations for them, to eating disorders, self-injury and so forth. So algorithms obviously have a powerful part to play on Instagram and Facebook and social media. We are going to pursue this issue.

I am drafting legislation on it. One of her recommendations was that there should be more transparency, more disclosure about how algorithms work, more oversight into this aspect of the internet. So my question to you, Professor Felten, is and to others who want to make observations, what should we be asking Facebook to tell us about their algorithms? What specific should we be demanding of them?

Mr. FELTEN. Sure. So an algorithm like Facebook's is extraordinarily complex. I think the conceptual handles one can get on it are maybe three things. One is, which data go into the algorithm, what is it using, and then any issues around accuracy or nature of that data? That is number one. I think number two is, what is it that the algorithm is trying to optimize or maximize? These machine learning algorithms are all trying to maximize some metric or measure of something.

With Facebook, it is maybe something like engagement, how often people click or time they spend on the site. And then what are they doing to understand the consequences? It is not simple to understand the consequences of one of these complex algorithms in operation.

But companies are constantly monitoring, measuring, evaluating how these things go, and getting a picture into what they are seeing internally on their dashboards or reports. It seems quite important for understanding what is going on.

Senator BLUMENTHAL. I am assuming you would agree that algorithms can be made safer in terms of protecting children and protecting data?

Mr. FELTEN. Absolutely.

Senator BLUMENTHAL. Would you have specific recommendations based on what you know about Facebook or Instagram's algorithms on what they should be doing.

Mr. FELTEN. With respect to children, the obvious first question is, should children be interacting with these technologies at all or interacting as part of the same broad system that adults are? In addition, I think the companies have at least an ethical responsibility to take special pains to understand how what they are doing impacts children.

What are the behaviors of children on this site? Because it is very difficult for anyone else, such as parents, to really govern this behavior if the company is not there taking basic precautions.

Senator BLUMENTHAL. But parents don't have the ability to change the algorithm, do they?

Mr. FELTEN. No, all they can do is look over their kid's shoulders or cut them off entirely.

Senator BLUMENTHAL. And in fact, my guess is that most parents have no idea what an algorithm is or what its effect is on their children.

Mr. FELTEN. Even I, as a parent of a once a young child, didn't really understand what these algorithms would be doing to my child. It is a lot of guesswork.

Senator BLUMENTHAL. So a good place to start for Congress might well be to require greater disclosure and transparency about algorithms. And if we were to establish, for example, an oversight board, it would be the work of that board to enforce greater safety to protect children.

Mr. FELTEN. I think understanding is a first step. And then thinking about how to govern these algorithms is extraordinarily difficult but important.

Senator BLUMENTHAL. But if Mark Zuckerberg is really serious about transparency, he would provide more disclosure about his algorithms.

Mr. FELTEN. There is certainly more they could do in terms of disclosure.

Senator BLUMENTHAL. Thank you.

Ms. RICH. Can I just add that I don't think it would be very useful for the disclosure to be to consumers. Because I don't think in the same way consumers don't read privacy policies, they are not going to look at all this programming and figure out how the algorithm works. So if there is going to be oversight, I think it should be Congressional oversight or agency oversight, but not disclosures to consumers unless it is—you are able to boil it down to something consumers can really understand.

Senator BLUMENTHAL. In the same way that the FDA regulates drugs or tobacco, for example. You would need some kind of oversight agency that had that specialized knowledge?

Ms. RICH. If Congress wants to regulate this, it needs to do more than have it be an ethical obligation. Yes, there needs to be some structure in place.

Senator BLUMENTHAL. Thank you.

Mr. LEE. Access to this data and information by independent researchers who truly are experts is also valuable.

Senator BLUMENTHAL. Very good point. Thank you.

The CHAIR. Senator Moran.

STATEMENT OF HON. JERRY MORAN, U.S. SENATOR FROM KANSAS

Senator MORAN. Chairman, thank you. Please take note of my indulgence and remember that. I am pleased to be here and appreciate this panel and this topic of conversation. This—as Senator Blackburn said, this has been a week of useful and valuable time spent in the Commerce committee. I don't know how to narrow my questions, and I have several and I want to get to one in particular, and I am saving it to last, which is probably a mistake.

But let me first of all, say Senator Shaheen and I are the appropriators for NIST, which are the ranking, Republican and back—and so my question maybe attended for Mr. Lee is, how can Con-

gress better equip NIST to provide effective cybersecurity guidance to organizations?

Mr. LEE. Well NIST does an amazing job, as you well know. And they provide, you know, great guidance that can form the basis of many of these enforceable standards that we are talking about. You already have some States now that are trying to make that easy to do. And if you do that, then you are relieved of some obligations and some liability under State law. So NIST is a great partner for what we have been talking about today. If we empower the FTC, the way it needs to be empowered, with the resources, with the personnel and with the mandate, it has to be in concert with NIST.

Senator MORAN. I am also an appropriator for the FTC. Let me ask, maybe this is for Ms. Tummarello. Our data—our Consumer Data Privacy Act, Privacy and Security Act, we try to scale the requirements based upon size, complexity, and the resources covered—resources of the covered entity or provider, as well as the sensitivity of the data. Tell me, in formulating comprehensive data privacy policy, how can Congress properly calibrate the data security requirements to ensure that tech startups aren't harmed, that we don't stifle innovation?

Ms. TUMMARELLO. Thank you for the question, Senator, and I appreciate the focus on not stifling startups' innovation. I think, you know, a guidance would have to be—requirements have to be nimble. And I think the suggestion of having the FTC issue annual guidance is a good one. Something that allows not only the cybersecurity threat landscape evolving, taking that into account, but also kind of the capabilities of startups. As those both evolve, the guidance will need to change. And so giving the FTC rule-making authority and then a requirement to issue updated guidance annually or something like that would be a huge step to provide startups clarity but also evolve with changing technology.

Senator MORAN. Maybe there is a point that you are making, which I would highlight, at least for me and others, is not just the nature of the regulations, not just the magnitude, but also the certainty. Certainty is hugely important. On this topic of certainty, as you and others may know, I have been engaged in negotiations, which I have answered every press person's question and every interested party's question that we are this far apart on getting something done.

But I have been saying that now for 2 years. I think what we heard yesterday, what is going on in the country, the states' enactment, international activity means that our work is more important maybe than it was when we started it. So the crux of the challenge is a desire for certainty and a nationwide standard. And then the other kind of issue that comes together is a private right of action. So the two things that keep pulling us apart are these two.

I would ask you, Ms. Tummarello, is there something that can be—that would be satisfactory, in—if the certainty of a national standard was provided, preemption, what is the ideas that we ought to be discussing to try to find common ground on the issue of liability or private right of action?

Ms. TUMMARELLO. Thank you. I think, you know, private right of action does get to the certainty question. It is not just—

Senator MORAN. They are not separate. You are right.

Ms. TUMMARELLO. Yes. And so having courts across the country issue different rulings is a huge issue that creates another patchwork for startups to comply with. And that is—that is kind of baked in to needing certainty. So I think there are ways to scope a narrow private right of action, especially around, you know, things like whether or not they have had notice and the opportunity to fix the problems. If there are specific harms, we are worried about making sure that is what the private right of action is focused on.

There are ways to scope it such that you mitigate the chance of bad faith litigation. But startups are especially vulnerable to bad faith litigation. We see it in other contexts, especially around intellectual property. And so making sure Congress is trying to put guardrails on a private right of action, I think is really critical.

Senator MORAN. I was going to ask others this similar question, but I am happy to do that, although my time has expired. And I don't know whether Senator Markey has become the Chairman of the hearing or not.

**STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS**

Senator MARKEY. Yes, through a miracle of a paucity of attendance, the chairmanship has devolved to me for a very brief, a fleeting moment in time.

Senator MORAN. And for which you have a conflict of interest because you are the next Senator to ask questions.

Senator MARKEY. And I recognize myself for as much time as I might want to consume on this incredibly important subject. So let me ask—you know, questions I have asked over and over and over again because any comprehensive cybersecurity regime must address the unique challenges created by the Internet of Things, the IoT.

And the Internet of Things includes all of the Internet connected devices increasingly prevalent in our everyday lives, such as connected refrigerators, laundry machines, dryers, baby monitors, smart locks with as many as 75 billion, can I say that again, 75 billion Internet of Things devices projected to be in our pockets and homes by 2025. The Internet of Things will also stand for the Internet of threats, until we protect this omnipresent technology from hacking and cyber intrusions. That is why I introduced the Cyber Shield Act with Congressman Ted Lieu, legislation to create a voluntary—can I underline that—voluntary cybersecurity certification program for Internet of Things devices. Our bill establishes an expert advisory committee to create cyber security benchmarks for Internet of Things devices.

Manufacturers can then voluntarily certify that their products meet these benchmarks and display this certification to the public with a Cyber Shield label akin to the Energy Star for energy efficient appliances that will help consumers identify and purchase more secure technology. I am very proud that President Biden included a new Internet of Things labeling pilot program that mirrors my Cyber Shield Act in his May 2021 Executive Order on cybersecurity.

Dr. Felten, do you agree that we should make an Internet of Things labeling program a permanent component of our Nation's cybersecurity safeguards by passing my bill?

Mr. FELTEN. Yes, I think having a permanent program of that nature would be—would certainly be helpful. There is an old saying that the problem with many of these devices is you can't tell if it is secure by looking at the box. And having a label that can be on there that consumers can recognize and having people be able to count on that into the future would be valuable.

Senator MARKEY. OK, great. And Ms. Tummarello, same question. Would that labeling program be helpful?

Ms. TUMMARELLO. Yes, absolutely. And I think the fact that it is voluntary is appreciative. And then it would allow startups to compete on security and privacy by saying we are certified, which could make it easier for them to get in consumers' hands. So I appreciate the idea.

Senator MARKEY. Yes, and you know, an energy star works. People can just see, oh, it is less expensive, and I get less efficiency out of this energy device as well. Or when you are buying a car and say, oh, it is only has two stars for safety and I have three young kids, maybe you have a car that has three or four or five stars here. You know, let me see. Just so you can have that kind of transparency.

Well, the same thing is true for all Internet of Things devices. People are just going to want to know and then they can make up their own minds. It is all voluntary. But at least they have the transparency of the information that allows them to make the decisions to protect their children or protect their own privacy by buying a higher standard. But just leaving it to an individual consumer to figure that out is obviously ultimately going to be very difficult to navigate. And I am also particularly concerned about cyber threats to children and teens' data. And that is why I reintroduced my bipartisan update to the Children's Online Privacy Protection Act.

The bill includes key data security protections to help kids and teens safely navigate the online ecosystem. Specifically, my legislation would require children's websites and apps to employ strong safeguards against hacks, require kids connected devices to meet robust cyber security standards, and require manufacturers to clearly communicate to consumers how they are protecting kids' data. So, Ms. Rich, do you agree that we should enact heightened cybersecurity protections for children and teens online?

Ms. RICH. Absolutely.

Senator MARKEY. Yes. Thank you. Dr. Felten, same question.

Mr. FELTEN. Yes.

Senator MARKEY. Ms. Tummarello?

Ms. TUMMARELLO. Yes, as long as we are not encouraging general audience services and products to collect more information to try to suss out if they have children. As long as this is child directed, I think that makes sense.

Senator MARKEY. Child directed. Yes—Mr. Lee.

Mr. LEE. Absolutely.

Senator MARKEY. Yes. Thank you. And so again, that is why Senator Cassidy and I have introduced this legislation. We just carve

out a special category of kids, provide them the protections, and what we do with adults, we will see, you know, but at least for children, they should have that safe harbor, you know, to grow up and not be concerned, especially parents, what is happening to the kids. So thank you. Let me turn and recognize the Senator from Florida, Senator Scott.

**STATEMENT OF HON. RICK SCOTT,
U.S. SENATOR FROM FLORIDA**

Senator SCOTT. Thank you, Chair—are you Chairman Markey—are you the Chair?

Senator MARKEY. I have the title for a brief period of time. I am like—I am like King John waiting for King Richard to return from the Middle East. So for the time being, I have it, yes.

Senator SCOTT. Thank you. Recently, the Biden Administration and Democrats in Congress have embraced a radical new policy that should terrify every American. Under Joe Biden's America, the Federal Government's authority would be vastly expanded, so the IRS would get a look at any account over \$600. The madness doesn't stop there. This new rule from Joe Biden will also require banks to report every transaction of \$600 or more. I completely oppose this disastrous proposal full stop. But to make matters even worse, the Federal Government can't even be trusted to keep the data it already collects safe. As we all know, in 2016, the IRS was the subject of a massive data breach.

Now, President Biden wants the IRS to have a data on the financial transactions that nearly every American family. You might expect this would come from communist China or Cuba, but a surveillance state is not something we should put up with in the United States. I have never—I have only been up here two and a half years, I have never gotten as much feedback from my constituents. I have heard from more than 18,000 Floridians on this issue alone in 2 weeks.

So here is my question. Do any of you believe the Federal Government is adequately prepared to protect the private financial information of millions and millions of Americans in a massive expansion of its current data holding capacity? And how can we expect hackers to not have a field day if the IRS, which is already a woefully unresponsive—is woefully unresponsive as a Federal agency gets this new authority? So what do you all think?

Ms. RICH. I am not an expert on Government security. I really worked on commercial area. But being a victim of data breaches affecting the Federal Government as a former Government employee and also working in an area where you know, we observed a lot of Government security problems, I do have concerns about the Government's ability to safeguard data.

Senator SCOTT. How about everybody else?

Ms. TUMMARELLO. Yes, I think there are concerns across the board about the Government's availability to safeguard data.

Senator SCOTT. Anybody feel comfortable with all your data being held by the Federal Government? Come on. There is no yeses, I guess. Alright.

Ms. RICH. I think we said yes.

Senator SCOTT. Every company looking to communist China is required by law to turn over any information their communist Government demands. How can we be sure that data stored in companies based in adversarial countries like communist China is protected?

Mr. FELTEN. There is a limit—there is a limited amount we can do, if anything, to protect that data. So we should absolutely be concerned about where our data is going, and what protections exist. They are both under the local law, but also in practice in those places.

Senator SCOTT. Anybody else? So what limitations we put on American tech companies that do business in communist China to make sure that information about Americans stored in a foreign country—what sort of limitations do you all recommend?

Ms. RICH. I would—if you decided to regulate American companies and they stored U.S. data abroad, I think technically there are legal theories for—that they need to protect that data even if it is kept abroad. Implementing that, bringing enforcement against them for that is the more difficult task.

Senator SCOTT. Anybody else? Thank you.

Senator MARKEY. So thank you, Senator Scott. And I think Senator Rosen is—

Senator ROSEN. I am here, Senator Markey—

Senator MARKEY. I recognize the Senator from Nevada.

**STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA**

Senator ROSEN. Thank you so much, Mr. Chair, appreciate it, and like my colleagues before me, everyone is trying to work on this issue, so I don't want to hoarder some of the bills that I have introduced to enhance data security. I would like to just address one. They are aimed at strengthening our cybersecurity capacity, providing cybersecurity resources, education to small businesses, to schools, local Governments. So like I said, one such bill I have Improving Telework Cybersecurity for Small Organizations Act. That would work to strengthen the cybersecurity capacity of small organizations to defend against telework related cyber threats through collaborative guidance and support from CISA and the FTC. We know telework, of course, has increased so much because of the pandemic, and I think a lot of that is here to stay, so I just want to bring that up.

But we also need to think about protecting our data through our cloud services because as more and more of us have to store data, we want to keep it safe and secure. Adopting cloud services we know can strengthen data security. It is going to provide a more resilient source of data sourcing. 90 percent of companies that have taken advantage of these benefits, and they are now on the cloud. But while migrating to cloud services provides a more resilient source of data hosting, it concentrates critical data, maybe in a small number of entities.

Last week, leaders in the cloud computing industry created an initiative aimed at establishing trusted cloud principles, basic commitments and protections for companies to store and process their data on the cloud. So Mr. Lee and then Dr. Felten, can you discuss

the unique data security challenges facing the cloud computing industry? Mr. Lee, first.

Mr. LEE. Thank you for the question. It is an issue for victims because increasingly, as we do move to the cloud, not every organization has the same level of robust security in place. So any effort to have more uniform standards around what you need to do for security would be welcome. I noted in our report from the—our data breach analysis from this last quarter, nearly 100 million individuals were impacted by the fact that organizations failed to add a password to their cloud environment.

It is basic blocking and tackling in many cases that compromises people's information. It is the lack of basic blocking and tackling, if you will. So it is an important issue, and it is something that needs to be addressed in a way that is enforceable. So if someone does fail to add that password, not very tough, but at least add that password, then if they fail to do that, there should be some enforcement action.

Senator ROSEN. Good cyber hygiene always helps. Thank you. Dr. Felten, could you address some of the unique challenges, and then I want to move on to talk about some resiliency and redundancy issues in the cloud.

Mr. FELTEN. Sure. There are a lot of advantages to organizations, especially smaller ones, relying on cloud services rather than trying to do things in-house. As you said, it does concentrate some of the vulnerability, but cloud companies can be central to sources of more cybersecurity expertise and better practices. They can really—they can really give the issue the attention that it needs.

The kind of standards and coordination that you talked about, I think, are really important to make sure that not only that the companies are—the cloud companies are doing what they can, but also their clear expectations about what the responsibilities of the cloud company versus their customers are so that things don't fall in between and get neglected.

Senator ROSEN. Thank you. Because I want to move on again, Dr. Felten, with the security implications again of a concentrated cloud service market. We not just have—we don't just have cyber security but also have physical security. I want to remind people the cloud is not really in space. The cloud is often warehouses and warehouses of servers, and so we have physical security to worry about. So how do we build resiliency and redundancy to minimize downtime and outages, not just in the cyber space for the cloud, but also perhaps in the physical space?

Mr. FELTEN. Sure. And as you know, there is no simple recipe for this. Redundancy is especially difficult when you are operating at this very large scale because you don't have much opportunity to try it out. It is an area that the largest cloud companies are putting a lot of attention into. They don't always succeed. We saw downtime from Facebook this week that was due to exactly the kind of failure that you were talking about.

So even the biggest and most sophisticated companies don't always get this right. I do think it is something that needs attention from the companies. It is an area where Government has expertise about defenses and about the threat landscape, which can be really valuable. And so there is a role that Government can play as well

in helping companies to figure out how to be as resilient as they need to be.

Senator ROSEN. I think you are exactly right. Things like parallel processing, mirror image systems, those things can really help. Thank you all for being here today and I see my time is up. Thank you, Mr. Chair.

The CHAIR. Thank you, Senator Rosen. And thank you for that line of questioning. I know we have several other members who still want to ask questions and are on the way from the vote, so I am just going to ask a second round while we are waiting for those senators to show up and then hopefully you guys can go on your way. I know it is been a long morning already and I know it is a little chilly in here.

I wanted to go back to Senator Cruz's question. You know, he was asking about other Federal agencies and our own data security issues. And I know now a couple of members have had discussions with you around NIST. So one, why isn't the FTC just good guidance for the rest of the Federal Government as it relates to data security? I mean, I look at NIST as a standard setting, but they are certainly not the policeman on the beat, and we are not asking the FTC to be the policeman on the beat for all of the Federal Government, but I guarantee you are definitely not going to get that out of NIST.

So here we have this burgeoning issue of cybersecurity for us as a nation, and we need to build our own capacity. We need to build our own capacity of a very technical, skilled team. And if you ask me, I have found that there are people in the boughs of organizations who are very, very technical. And then I know people at the very high ends of operations in various aspects of the Federal Government who are also very knowledgeable and very technical. But I see a gulf of people in between who aren't.

And that is the most frustrating thing. So could the FTC—what do you see this role—do you—are you back to this notion of we are just going to have to find somebody else to be the Government enforcer here to make sure that agencies are doing the oversight?

Ms. RICH. I think what I meant wasn't that the FTC can't provide guidance. In fact, the FTC has been brought in by OPM and OMB to help when there have been breaches to deal with the aftermath because of their expertise. But so I think the FTC could work with NIST to provide guidance for the Federal Government and there may be others, you know, cybersecurity folks that would participate in that too. What the FTC can't do is make the other agencies follow it because it is just a lateral agency.

And I was in the trenches long enough, with squabbles between the agencies and to know that that is just not workable. But the FTC could certainly help provide leadership and guidance that OMB could then push down to the agencies.

The CHAIR. OK. Anything else, Dr. Felten on that? So another point that was brought up. So, Ms. Rich, on—when consumers have been harmed, you believe in their common law rights to sue and to have damages and—correct?

Ms. RICH. I generally do believe that, absolutely. But I am speaking, you know, practically about—because it is been such an intractable issue that if you have a really strong law, sufficient resources

to enforce it, 50 State AGs on the beat too, that that would be a very good outcome, much better than we have now and could mean we don't need to have a private right of action, especially since private rights of action can complicate an already complicated issue.

The CHAIR. Well, I would beg to differ on that from a global perspective. I think yesterday was a perfect example of how you can—if you don't have real damages that someone is going to feel in these situations, you are going to have a lot of behavior that just continues. And just like on the data security side here, we again, Mr. Lee has been very crisp and clear about the amount of damage that is being done to consumers.

But when you think about these organizations across the board, they are not paying the price. I guarantee you that Equifax had nowhere near the damage done to it as the individuals did, if you were looking at it in a comparison. I mean, when people lost their homes, lost their jobs, lost their health care, lost these things, it has been pretty significant.

So I would just hope that we will certainly get to you with some questions about what you meant on those middle ground issues. But I am going to turn to my colleague, Senator Peters.

**STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN**

Senator PETERS. Well, thank you, Madam Chair. Thank you for this hearing and a very important discussion. I want to thank each of our witnesses for being here. First of all, I just want to echo my colleague's calls that we have heard here in committee for increased reporting on data breaches and how important that is. Actually, just moments ago, where I just came from, the Homeland Security committee where I chair, we just marked up a bipartisan bill that I sponsor that would require certain entities to report substantial cyber incidents to CISA. And included in that, of course, are major data breaches.

I certainly think this bill will address some of the challenges that have been mentioned today, although we know there are many more. I have also introduced legislation in this committee, the Data Broker List Act, which would require data brokers to have in place comprehensive information security systems to prevent those data breaches from happening in the first place. We want to be on the front end, certainly.

My first question is for Mr. Lee. When we think about ransom attacks, we know that they have become increasingly common, and data security legislation has to certainly limit these illicit acts. As an example, in 2020, Ukrainian hackers targeted a health care company with locations throughout Monroe County in Michigan, and in order to unlock stolen patients and financial data, they had to pay over a \$30,000 ransom.

So my question for you, Mr. Lee, is, can you give me examples of data security standards that would have the most impact in trying to prevent ransomware attacks from occurring in the first place? What would you suggest that we really focus on?

Mr. LEE. It really all begins with, let's prevent the data breach because ransomware attacks are fueled by data that has already been stolen. So if we can prevent that from ever happening for the

most part, then you are going to have a tremendous impact downstream. You won't have as many ransomware attacks.

You will still have them because there is multiple ways of doing it, but you won't have what you have today where largely ransomware attacks are committed because someone has a log in and a password and can infiltrate a system, or the SolarWinds attack, which was because of an administrator's password that had been acquired.

And then it was a weak password to begin with, so that didn't help. So if we can prevent those breaches from ever occurring because of stronger cybersecurity standards that are enforceable, we will get to ransomware.

Senator PETERS. Well, that is good to hear. Well, my bill, the Data Broker List Act, would require data brokers to have in place a comprehensive information security system to mitigate that risk that you mentioned, Mr. Lee. And because of the role that data brokers play in today's data marketplace, it seems to me it is critical that regulations address their storage, their use, and certainly as you mentioned, the security of their data.

Ms. Rich, how do you believe data brokers should be addressed if we are looking at comprehensive data security legislation? Could you be specific about data brokers?

Ms. RICH. The opposite—in the same way that that Dr. Felten talked about social networks, it being a matter of degree because they have so much data, the same can be said about data brokers and their whole business is data.

So they have got a lot of it, and they have to, in terms of scalability, they would be at the top of the scale of protecting information because they also have a lot of sensitive data. Of course, for data brokers, privacy is a critical issue too. I mean, just as critical.

You know, when can they—what kind of vetting do they need to do? Who can they sell the data to? Are they sure when they got the data that it wasn't subject to, you know, controls, et cetera? So privacy is a huge piece of the data broker story as well.

Senator PETERS. And a follow up to that, what other tools that we could provide to the FTC to actually enforce standards that are in place for data brokers?

Ms. RICH. If there were standards in place for data brokers, then all the tools that the Chair Cantwell is trying to provide to the FTC, more resources for technologists, for attorneys, for this new privacy bureau would be extremely valuable—essential. But there need to be standards in place because there aren't any.

Senator PETERS. Yes, you have to start with standards, but you also have to make sure those standards are followed and enforcement. It is a two-step process that is both critical, as you well know. Well, the Michigan patients that had their financial data stolen, as I mentioned earlier in my comments, were given free credit monitoring service after that, but their data obviously was already compromised, already a big issue.

So, Mr. Lee, I know you noted in your testimony a study by the University of Michigan that showed that we are not equipping victims with the information needed to protect themselves. What are some of the most effective ways in your mind to support victims of

these identity crimes? Is there something we are not doing now that we should be thinking about?

Mr. LEE. Well, first of all, we should be more transparent in what we tell people. The Michigan study, along with the Carnegie Mellon study, make it very clear that the—literally the language we use in the notices is so dense, people don't read it.

Senator PETERS. Right.

Mr. LEE. They don't even realize that they have been breached not once, not twice, three and four times, and they don't know it. And so they basically they don't do anything. There are very basic steps that people can take that we should tell them about, but we don't. And we are not—because of the patchwork of State laws, each one being a little bit different, each one has a different form and both substance, so something as simple as, while credit monitoring is great, a credit freeze is better because a credit freeze means no one can open an account with your information. They can't—they cannot incur debt on your behalf.

A credit monitoring, while it is helpful, it tells you what has happened. The horse is out of the barn. We don't need just that. We need a lot more robust kinds of information and—that we give to consumers. We give to victims. And we need to do it ahead of time, too. So that is a different conversation, but the whole concept of a victim support structure that is lacking in this area of identity crime—we can prevent a lot of it, and we can equip people to prepare them for it when it does happen.

Senator PETERS. Right. Thank you. Thank you, Madam Chair.

The CHAIR. So do we have Senator Warnock, remotely? OK. And we still may be waiting for one more senator. I wanted to ask you, Ms. Rich, on your testimony, written testimony. I am not sure if you mentioned it in your oral testimony. You were talking about common carriers being under the FTC instead of the FCC. Would you elaborate on that?

Ms. RICH. Well, I didn't say instead. I didn't say that. But I do—

The CHAIR. OK—on privacy and data.

Ms. RICH.—I do believe that it would be important to create a level playing field, both for consumers and for businesses, if you have a data security law. And so for that reason, covering non-profits and common carriers and allowing the FTC with the new resources you are giving it to bring enforcement would be very important. As to the FCC, I don't think they have been particularly active in the data security area.

I mean, if you were going to switch it over, I would have to look at a provision and give—you know, see whether it would reduce any protections that exist now. But I don't think this has been an area where the FCC has been active or has particular expertise. I think the FTC could do an amazing job with the resources you are going to give it on data security—and the authority you are going to give it on data security.

The CHAIR. Dr. Felten.

Mr. FELTEN. I agree. The FCC is good at what they do, but I think having that—having that level playing field and allowing the FTC to not face these sort of artificial boundaries in how it does enforcement, would be valuable.

The CHAIR. Mr. Lee, did you have any comment on this point? I know it might not be your area, but you might have seen cases in here. No. OK.

Mr. LEE. No.

The CHAIR. Alright.

Mr. LEE. Thanks for asking though.

The CHAIR. Thank you. Well—

Ms. RICH. Could you give me 30 seconds to just address the private right of action, again?

The CHAIR. Yes.

Ms. RICH. Because I think you think I don't care about consumers and their rights. My point was just that the if you—with the proper resources and authority, the FTC and the states could also represent consumers and get money back for them, redress, civil penalties, whatever is appropriate, if the law is strong enough and it gives the remedies. That was my point.

The CHAIR. So again, not to put words in your mouth, but you are saying, yes, if consumers are harmed, they should be able to get actual damages. The question is what process should they be able to get actual damages?

Ms. RICH. Yes.

The CHAIR. And so I think that is going to be a big discussion point among us as well. And so I really appreciate your input on it. So but I just I didn't think that you didn't. I just wanted to make clear that this actually is the issue. And when you look at yesterday, you, in my opinion, you look at how do you create bright lines within big organizations, how do you have out there in the public and within these companies, because you don't have a CFO or CTO or even the general counsel running around every day saying these are the do's and don'ts, but you do, if there is a strong law, and you know that the company can be held accountable for it. That is the kind of thing we are looking for.

And we have to build in—as my colleague, Senator Klobuchar was saying, this is like an entire growth area of our economy. And we want it to succeed. I sit here and listen to—there are a lot of good algorithms, trust me. A lot of—there are a lot of algorithms that are helping us even today. So yes, now we have a lot of people who are going to understand what algorithms are all about. But the point is, we have to have some bright lights—bright lines here.

And as much as I want a powerful FTC, I think that Europe still fails to get the job done. We kind of know what that looks like. We can see what the European model is accomplishing, and we can see that it has shortcomings. So we know this, that as Mr. Lee was saying, that if you can have these people be accountable to their—the damage, the same kind of damage that is being done to consumers, you are going to get a better response in policing them. And the information age is going to continue to change.

So this committee has been very prescriptive. I would say, for 15—the amount of time I have been on this committee, very prescriptive. So that is where it has gotten us. So the information age is growing by leaps and bounds and each little sector we have tried to be prescriptive, and I would say, have we accomplished what we have wanted to accomplish? I would say no, given Mr. Lee's data and given what we just had yesterday. I would say we need some—

thing stronger. We need a very bright line on accountability. But anyway, we will get to this discussion with our colleagues.

And hopefully—I think the one thing people who have been watching these hearings will see is that we have a very engaged committee. And it doesn't matter how many cameras are outside that door, OK, because you had a lot of people here and a lot of people last week asking and knowing the subject area. They are drafting or have drafted legislation in this area.

Practically every member of the Committee has been on one form or another of these legislations. So I do think the moment is here. And again, just thank you all for your expertise. This is very, very helpful. And I think that hopefully our colleagues will come together at this moment, and we will be able to get some legislation to help bolster and protect consumers.

So with that, the hearing record will remain open for 1 week until October 13, 2021. Any Senators who would like to submit questions for the record should do so by that date. We ask that responses be returned to the Committee as quickly as possible, but no later than October 27, 2021. So with that, the hearing is concluded.

[Whereupon, at 12:24 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO
JAMES E. LEE

Cybersecurity Literacy. We must educate Americans on how to identify and react to cyber threats. For example, it's important for everyday Americans to be able to identify a phishing scam. 91 percent of all cyberattacks begin with a phishing e-mail. My bill with Senator Thune, the *American Cybersecurity Literacy Act*, aims to improve cybersecurity literacy by requiring the National Telecommunications and Information Administration to conduct a cybersecurity literacy campaign to increase knowledge of best practices to reduce risks.

Question 1. In your testimony, you note that phishing attacks are the most common form of cyberattacks. Can you speak to the importance of educating Americans on how to identify and avoid cybersecurity threats?

Answer. Thank you, Senator Klobuchar. As the only national non-profit that directly supports identity crime victims and provides education resources to help consumers from becoming victims (all provided free of charge), the ITRC could not agree more with your statement and the goal of your bill with Senator Thune. While the focus of the October committee hearing was to improve cybersecurity as a means of protecting consumers and businesses, the reality is much more is needed, including a comprehensive and sustained effort to both equip consumers with the tools needed to protect themselves and support services when their identities are compromised and/or misused.

Since the committee hearing, the ITRC has published research that shows consumers and *small businesses* are repeatedly victimized at an alarming rate. Yet, only three percent (3 percent) of consumers take the most effective action to protect themselves from identity crimes: freezing their credit or using different passwords on every account—even though nearly 80 percent of consumers admit they know about credit freezes, and only 15 percent claim they have unique credentials for every online account.

More than one million consumers come to the ITRC's website each year to learn about the latest identity scams and how to avoid them or recover from them. We would welcome the opportunity to help even more people avoid becoming a victim. Providing the NTIA with the ability to award grants to organizations that provide identity protection, without charge, would be a welcome addition to the victim prevention landscape.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KYRSTEN SINEMA TO
JAMES E. LEE

State Privacy Laws. Like many states, the Arizona state legislature has considered implementing a consumer privacy law. Three states—California, Colorado, and Virginia—have enacted their own privacy legislation.

Question 1. Do you believe Congress should enact a national consumer privacy law? If so, what are the key elements of a Federal data privacy law to protect Arizonans, especially in regards to data security?

Answer. Thank you, Senator Sinema, for the opportunity to expand on the ITRC's earlier testimony.

In short, the ITRC believes identity crimes and, as a result, the number of identity crime victims would be reduced with the adoption of comprehensive, enforceable data security and privacy standards. As you note, states are already adopting a unified approach that combine privacy and security protections into a single legal framework. In the absence of a Federal law, states will continue to adopt their own standards resulting in the same inefficient patchwork of laws we see today with data breach notice requirements. I would point you and the staff to our response

to the Minority members' questions where we provide a detailed discussion of state laws.

The result of the state-by-state efforts is identity crime victims having different protections and different remedies to the same event depending on where they live. As we pointed out to Senator Wicker, without a uniform national definition of what is considered "personal information," a resident of Mississippi whose passport, military ID, or biometric data was breached would not be required to be notified of a compromise of that information, yet someone across the state line in Alabama would because the two states define personal information differently.

The ITRC believes the core elements of any national privacy law can be found in the California, Colorado, and Virginia state laws: Right of Notice, Right of Access, Right to Delete, Right to Correct, and Limited Right to Opt-out, and Data Minimization. We also believe consumers are well served by mandatory privacy and security audit provisions found in the new state laws as well as the cybersecurity regulations of the New York Department of Financial Services (*23 NYCRR Part 500—Cybersecurity*). There should be a robust penalty provision for violations balanced with incentives for compliance—a Safe Harbor for good faith efforts to comply, for example.

Question 2. How should a Federal data privacy law interact with state data privacy laws?

Answer. The ITRC believes that identity victims and the public at large are best served with strong, enforceable minimum standards at the Federal level. However, technology in general and cybercriminals in particular move faster than Congress can respond with new laws. Allowing states the flexibility to rapidly respond to new and emerging threats is important to ensure consumers and businesses are well protected.

FTC Resources. Unfortunately, Arizona schools, hospitals, and companies have been the victims of cyberattacks that have resulted in the release of personal information. Since 2005, data breaches have cost Arizonans at least \$1.6 billion.

Question 1. Considering the costs of these cyber incidents to Arizona and the Nation as a whole, what are your thoughts on providing additional resources to the Federal Trade Commission (FTC) to enforce existing Federal data privacy laws?

Answer. As a long-time partner of the FTC to whom the Commission refers complex identity crime cases for victim support, the ITRC supports providing the FTC with a clear enforcement mandate and the additional resources needed to fulfill its mission. We also believe there is an equally important opportunity to improve support services for identity crime victims by giving the FTC grant-making authority and funding.

Question 2. If you believe that additional funding is warranted, what is the appropriate amount of additional funding for FTC enforcement? Should that number be based on whether Congress passes legislation related to data privacy or data security?

Answer. The ITRC is not in a position to advise the Committee on the appropriate level of funding, but we do believe additional funding is required to adequately address the issues at hand. However, the need for additional enforcement and victim support should not be contingent on a Federal privacy and/or security law. The need for both enhanced enforcement and victim support is justified by the increasing number of cyberattacks, cyberbreaches, and business and individual identity crime victims.

Question 3. If a data breach involving their systems occurs, what types of services should companies provide to their consumers?

Answer. The ITRC believes that the current data breach notification system is ineffective and inadequate as we have noted in previous testimony and in response to questions from other Committee members. This includes the remediation services most often offered to victims.

However, the ITRC believes the most effective actions breached organizations can take to help victims include the following, several of which can be accomplished at no cost to the breached business:

- Consumers should be advised to freeze their credit with the credit reporting agencies and take the same action for their minor children. Credit monitoring offers no protective benefits.
- Businesses should force password resets for all impacted accounts and victims should be advised to reset passwords on every account with a unique, strong password using a password manager if needed.

- Businesses should provide identity remediation and restoration services in addition to credit monitoring for a minimum of five (5) years that should be renewed for an additional five years if there is evidence of identity crimes resulting from the compromised data.
- Beyond the breach notice, businesses should provide access to comprehensive identity protection education and remediation resources from independent sources. Research shows some consumers are deeply skeptical of paid services offered by providers affiliated with a breached organization, so offering a self-help or independent alternative is important.

The ITRC also recommends the form, substance, and delivery channel of breach notices should be reviewed in light of the emerging body of evidence that consumers are not taking appropriate post-breach protective actions. The current trend of businesses using website notices, news releases, or AGs notices instead of direct notices to consumers is having a detrimental effect on consumers and is increasing the risk of a ransomware attack or other compromise due to poor password management, especially at small businesses.

By way of explanation, the nature of identity crimes makes it difficult to craft “one-size-fits-all” solutions for victims which increasingly include small businesses and solopreneurs. The current practice of providing credit monitoring for one or two years is helpful, but not always adequate or effective. (Some states require credit monitoring for varying periods of time depending on the company, while some states do not require any monitoring or remediation be provided to consumers.)

Identity crimes, though, have a long tail where the compromised data can be used multiple times by multiple criminals over a period of years that may extend well beyond the monitoring period. As of 2021, 29 percent of victims contacting the ITRC were repeat victims who would not be protected by a one-year credit monitoring protocol.

Since the October Committee hearing, the ITRC has published research that shows more than 70 percent of adult consumers have received a data breach notice, yet only three percent (3 percent) take the most effective step needed to protect themselves from future identity crimes—a credit freeze. Sixteen percent (16 percent) take no action at all; Forty-eight percent (48 percent) only change the password on the account that has been compromised—even when 85 percent of consumers admit they use the same password on multiple accounts. Research from Carnegie Mellon University shows that most consumers replace a breached password with a weaker password, too.

Compliance Costs. Some tech companies have the resources to employ large numbers of compliance staff to ensure they are following national and state regulations. Many Arizona small businesses do not have access to comparable resources.

Question. How can we craft a Federal data privacy law that does not put small businesses at a disadvantage while still offering consumers strong data security protections?

Answer. The ITRC believes that adopting a strong, enforceable minimum standard will help small businesses—especially those who already commit to provide data and privacy protections for their customers, prospects, and employees—by leveling the playing field. Much of the inefficiency (and risk) in the current system is based on the patchwork of state and industry self-regulation requirements or lack thereof. Adopting a uniform, but enforceable, minimum standard ensures all small businesses play by the same rules. Minimum standards should take into consideration unique risks based on business size, data type, use, storage, and sharing/selling.

New businesses, in particular, should be encouraged to collect and maintain the least amount of data needed, thereby reducing the risk landscape.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RAPHAEL WARNOCK TO
JAMES E. LEE

Identity Theft. Every year, millions of Americans become victims of identity theft, costing them sensitive and private information and millions of dollars. Georgia has the seventh highest rate of reported identity theft in the country, and many incidents of these identity theft incidents stem from some type of data breach. In addition to the financial harm to working families, identity theft can also prevent these same families from accessing government resources to get them back on their feet, like stimulus checks, unemployment insurance, or child-tax credits. Although many states have their own resources and regulations to protect Americans from identity theft, I believe there is more Congress and the FTC can do to prevent identity theft and assist victims in recovering.

Question. What is the single most important thing Congress can include in legislation to protect victims of identity theft?

Answer. Thank you, Senator Warnock for the opportunity to talk about the need to assist identity crime victims.

Without a doubt, Congress can and should play a more active role in protecting identity crime victims. While the Committee is rightly focused in this proceeding on preventing identity crimes through data and privacy protections, these actions will only address half of the problem. By definition, though, there will still be identity crime victims who need support and assistance to recover from identity compromises like a data breach or identity fraud that results in the denial of a needed resources such as unemployment benefits.

Based on the most recent FBI, Department of Justice, and FTC statistics, there are more identity crimes (and crime victims) per year than all violent crimes combined. With a 29 percent revictimization rate, identity crime victims find themselves the subject of subsequent, repeat crimes more than any other offense types.

Yet, identity crime victims are not eligible for crime victim assistance funds from the Office of Victims of Crimes (OVC) programs. Identity crimes are not specifically tracked by the Bureau of Justice Statistic. Only 11 states allow victims to pursue private legal actions in the wake of an identity crime (AK, CA, DC, LA, MD, MN, NH, NC, SC, TN, and WA). In the past decade, the Federal government has provided less than \$10M dollars in three budget cycles for identity crime victim assistance. No state provides dedicated funding to identity crime victim assistance. Absent additional, dedicated resources from government and the private sector, there exists the very real possibility of no free, direct consumer support offerings in the next several years.

Direct identity crime victim assistance is available from only a handful of organizations—most of which are for-profit organizations. There is only one non-profit organization offering nationwide no-cost victim assistance, consumer and business education, and government agency tier-two support—the ITRC.

The ITRC believes Congress should pursue a model for addressing identity crimes that has proven to be successful in other areas of law enforcement. Specifically, the fusion center model adopted in the wake of the September 11, 2001, terrorist attacks.

A virtual Identity Fusion Center (IFC)—or “one-stop shop”—for addressing identity crimes and supporting identity crime victims would link local, state, and Federal agencies along with private sector entities such as data brokers, credit bureaus, financial institutions, and victim assistance groups like the ITRC in a single, virtual hub. Through a triage system, crime victims and curious consumers could contact the IFC to obtain advice or direct assistance from the appropriate agencies across multiple jurisdictions and geographic regions as well as non-profit and private sector organizations.

The ITRC is available to discuss this concept at your convenience.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROGER WICKER TO
JAMES E. LEE

Question. Today, all 50 states have enacted data breach notification laws. At least 25 states have laws that address the data security of private sector entities. Please answer the following:

Which state (or states) has the strongest breach notification law? Which state (or states) has the least effective breach notification law?

Why is it considered the strongest law? The least effective? Please explain and reference particular elements or features of the law.

Which state (or states) has the strongest data security law? Which state (or states) has the least effective data security law?

Why is it considered the strongest law? The least effective? Please explain and reference particular elements or features of the law.

Of the states identified above, which states have had the most success in preventing cyber incidents and/or responding to security breaches with respect to limiting consumers’ exposure to threats and reducing security risks to consumers’ data?

Answer. Thank you, Ranking Member Wicker, for the questions. There is a lot to learn from looking at the myriad number of state laws and regulations—some positive examples and some areas for improvement—as your question suggests.

As a preamble to answering your specific questions and as stated in our previous testimony, the ITRC believes the current state-by-state breach notification system is inadequate. With no uniform definition of Personally Identifiable Information (PII), triggering event, time-frame or method of notification, penalty for non-compli-

ance, or mandatory victim support, victims in different states impacted by a single data compromise are treated differently.

For example, a resident of Mississippi where the state law does not include passport or biometric information in the definition of PII would not be required to receive a notification if such information were compromised, but a person in Alabama would.

Next, state laws tend to fall into three categories: those which were passed in the wake of 2005's data breaches revealed by the California law; those passed after the data breaches at Target and later at Equifax; and those laws that have been amended over time to expand the definition of PII. For ease of reference for your staff, I have attached the compendium of state laws published by *PerkinsCoie* that was updated in September 2021 that provides code citations, effective dates, and dates of amendments.

You have asked the following specific questions:

Which state (or states) has the strongest breach notification law? Why is it considered the strongest law? Please explain and reference particular elements or features of the law.

It's difficult to point to a single state or set of state laws as being the "strongest" since even those laws which have strong provisions often have equally weak provisions, too. For example, a majority of states require residents to be notified of a data breach irrespective of how many residents are impacted—that's a strong provision.

Yet, many of those same states do not set a specific time-period for the notice—and still more allow the breached entity to determine if there is risk of harm from the compromise. No risk; no notice required; and no specific time-frame for issuing a notice. Those are weak provisions.

In the view of the ITRC, the following state law provisions should be considered for a Federal law:

Definition of PII

California—Cal. Civ. Code § 1798.29; 1798.82 *et seq.*

Personal Information Definition.

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted (meaning rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security):

- Social Security number;
- Driver's license number or state identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical information (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional);
- Health insurance information (an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records);
- Information or data collected through the use or operation of an automated license plate recognition system (a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data); or
- biometric data generated from measurements or technical analysis of human body characteristics (*e.g.*, fingerprint, retina, or iris image) used to authenticate a specific individual.

(2) User name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

California currently offers the most comprehensive definition of PII. Identities are not static and the definition of PII requires periodic updates to be effective.

Notice Provisions

Connecticut—Conn. Gen. Stat. § 36a-701b

Notification Obligation to Attorney General. Any Entity that is required under the statute to notify CT residents of any breach of security shall provide notice of the breach of security to the Attorney General not later than the time notice is provided to the residents.

Connecticut's provision is similar to requirements in other states, but Connecticut requires the Attorney General to be notified irrespective of the number of victims as opposed to other states that set a threshold—usually 500 to 1000 residents. At the Federal level, this requirement would provide a uniform data set for reporting purposes as well as an incentive to issue notifications when required.

Oregon—Or. Rev. Stat. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626

Notification Obligation. Any Entity to which the statute applies shall give notice of the breach of security following discovery of such breach of security, or receipt of notification, to any consumer to whom the PI pertains.

- Notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local agencies responsible for law enforcement, the Entity reasonably determines that the breach has not and will not likely result in harm to the individuals whose PI has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.

Oregon's notification provision is stronger than most states in that it requires an independent review of the risks associated with a breach. Most states only require the breached entity to make a determination that the breach "has not and will not likely result in harm" to victims who PII has been compromised.

As the nature of PII changes to include logins and passwords, it is increasingly difficult to determine "likely harm" resulting from a data breach. The volume of data breaches also makes it difficult to determine which data breach may have caused a particular harm. A provision similar to Oregon's reduces the chances of a well-intentioned, but ill-equipped entity misjudging the risk of their own breach.

Enforcement & Penalty Provisions

Forty-one states and the District of Columbia have enforcement and/or penalty provisions. Those states generally give responsibility to the Attorney General or other state agency to enforce civil penalties. Michigan imposes criminal penalties, too. Within the universe of states with enforcement provisions, 11 states have some form of a private right of action. No state without an enforcement mechanism offers a PROA. The eleven states are: AK, CA, DC, LA, MD, MN, NH, NC, SC, TN, and WA.

Enforcement by the state Attorney General is the most common scheme with most Attorneys General having the authority to seek injunctions as well as civil penalties and restitution. The following state laws offer strong enforcement and civil penalty provisions.

Arizona—Ariz. Rev. Stat. § 18-551 et seq.

Attorney General Enforcement. A knowing and willful violation of this section is an unlawful practice pursuant to ARS 44-1522, enforced by the Attorney General. The Attorney General may impose a civil penalty for a violation of this article not to exceed the lesser of \$10,000 per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed \$500,000.

Florida—FLA. STAT. § 501.171

Penalties. An Entity that violates the statute in the following manner is subject to the following administrative fines:

- A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the Department against an Entity or third-party agent.

- An Entity that fails to notify the Department or Affected Individuals shall be liable for a civil penalty not to exceed \$500,000 (i) in the amount of \$1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, \$50,000 for each 30-day period or portion thereof for up to 180 days; or (ii) if the violation continues for more than 180 days, in an amount not to exceed \$500,000. The civil penalties under this paragraph apply per breach, and not per individual affected by the breach.

Which state (or states) has the least effective breach notification law? Why is it considered the least effective? Please explain and reference particular elements or features of the law.

Any of the state laws that lack specific enforcement provisions. Without a specific enforcement and penalty provision or the private right of action, victims have no recourse in the event of a breach in the 10 jurisdictions that lack such.

Any of the states that still have narrow definitions of PII that often date back to the first series of data breach laws passed in the mid-2000s. For example, the most valuable PII to a cybercriminal today is a login and password, yet not all states define e-mail or account credentials as PII. The same is true of passports, military ID, biometrics, geo-location data, and other common or emerging PII.

All 52 state and territorial laws fall short when it comes to informing victims as to what happened, why, and what they can do to protect themselves. Breached entities are increasingly using the alternate notification methods allowed under virtually all of the state laws, which means victims are not receiving a direct notice. Here's a common example from an otherwise strong state law:

Oregon—Or. Rev. Stat. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626

1. *Substitute Notice Available.* If the Entity demonstrates that the cost of providing notice would exceed \$250,000, that the affected class of individuals to be notified exceeds 350,000, or if the Entity does not have sufficient contact information to provide notice. Substitute notice consists of the following:
 - Conspicuous posting of the notice or a link to the notice on the Entity's website, if the Entity maintains a website; and
 - Notification to major statewide television and newspaper media.

Which state (or states) has the strongest data security law? Why is it considered the strongest law? Please explain and reference particular elements or features of the law.

The trend at the state level is to take a more holistic approach to data security and privacy. While we've traditionally treated them as separate issues, the reality is they are interrelated—you can't have strong privacy without strong security.

Since 2020 three states that have adopted strong, integrated privacy and security laws and still more states have considered or are considering similar laws. One state, New York, has an especially strong and effective set of sector specific data security and privacy specific requirements for companies regulated by the state Department of Financial Services (23 NYCRR Part 500—*Cybersecurity*).

The principals found in the state laws of California, Virginia, and Colorado as well as those bills that failed in Washington, Oklahoma, and Florida (and are likely to be revived in the next legislative cycle) offer a good guide for a Federal law. All of these laws to one degree or another include the following principals: Right of access, deletion, correction, portability, and opt-out of data for marketing purposes as well as certain automated processes.

These laws also focus on data minimization—don't collect more information than is needed & don't keep it longer than required to complete a transaction.

There are also specific provisions that require routine cybersecurity and privacy assessments. These routine audits are also required by the NY DFS regulations cited above and have already led to both improved *cybersecurity and enforcement actions*.

Which state (or states) has the least effective data security law? Why is it considered the least effective? Please explain and reference particular elements or features of the law.

Most of these laws are so new and their provisions are so varied, it's difficult to tell how well they are or are not working. With the limited data available, there are no indicators—number of breaches, number of identity crime victims, location of

both—that point to a significant, positive impact that can be traced directly to any particular law or regulation.

Of the states identified above, which states have had the most success in preventing cyber incidents and/or responding to security breaches with respect to limiting consumers' exposure to threats and reducing security risks to consumers' data?

Frankly, the state data breach laws are all well-intentioned, but are not as effective as they should be. Given the research conducted by the University of Michigan and Carnegie Mellon University as cited in the previous ITRC testimony as well as new research by the ITRC, the notices generally fall on deaf ears and do not prompt consumers to take the very basic steps needed to protect themselves from harm.

In an ITRC survey of 1000 consumers, 72 percent acknowledged they had received at least one data breach notice. Of those respondents only three percent (3 percent) stated they had taken the single most important step following a data breach—freezing their credit—even though 80 percent said they were familiar with the process of freezing their credit.

As for cybersecurity, look to the pending legislation in Ohio that creates a Safe Harbor for organizations that adopt and follow the NIST cyber standards. If enacted, it will be fascinating to see what happens there.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO
JAMES E. LEE

Question. What can Congress do to make compliance with a new Federal law less complex, while still ensuring that companies are protecting consumers' data and privacy?

Answer. Thank you, Senator Thune, for the question. Businesses of all sizes that work across state and national borders are currently compelled to comply with a variety of privacy, security, and data breach notice laws. Depending on the type of organization and the sector in which the business operates, there can be multiple regulatory agency rules and regulations that compel compliance, too.

Applying a common, strong minimum Federal standard that is enforceable will actually result in less complexity for these organizations and better protections from cyber and identity crimes, especially for those residents of states with less stringent current laws. For the millions of small businesses that do not operate outside a single state or in a regulated industry, a common minimum standard will result in a level of certainty that does not exist today. It will also level the playing field for those businesses that operate with a high level of protection for their customers' data compared to those organizations that take a less privacy and security conscious approach to business.

When adopting a new, national minimum standard, Congress should look to those states which have already adopted strong, integrated privacy, identity, and cybersecurity statutes. Taking an integrated approach to what have traditionally been three separate legal silos also reduces complexity and increases the likelihood of compliance and efficacy.

The ITRC believes identity crime victims are best served when we prevent data breaches and cyberattacks from happening, and when they do, by ensuring the data that is available is benign. Therefore, we believe Congress should look to the principals found in the California and Virginia privacy laws adopted by the voters in 2020 and state legislature in 2021, respectively, as good guides for a national privacy and security framework. Specifically, the rights of data access, correction, limited deletion, and opt-out—easily exercised—coupled with the concept of data minimization—i.e. don't collect or keep more data than you need. Equally important are the requirements for routine privacy and cybersecurity audits to help ensure organizations subject to the law know and act upon any deficiencies that pose a risk to their business and customers.

What Congress should *not* do is adopt overly prescriptive approaches or preclude states from adopting innovative tactics in response to the constantly evolving attack vectors favored by financially motivated cybercriminals and Nation/State threat actors. The Federal Government, as well intentioned as it is, cannot react as fast as technology changes, so there must be a level of flexibility built into the system to ensure business and consumers alike can be protected from new forms of cyberattacks and cybercrimes as they emerge.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO
JESSICA L. RICH

Working with the Private Sector. The public and private sector need to work together to combat cyberattacks. Last year, SolarWinds—a commercial software product used by many government agencies—was revealed to have been hacked, resulting in a massive breach in computer systems across various parts of the Federal government and the private sector. The hackers were able to access over 18,000 government and private computer networks.

Question. In your testimony, you note that national security is at risk when government agencies use commercial software that is susceptible to hacking and other cyberattacks. Specifically, how should the government work with the private sector to improve cybersecurity?

Answer. To truly incentivize robust cybersecurity measures in the private sector, Congress should pass a Federal law requiring implementation of such measures by all U.S. companies (and, to the extent jurisdictional limits allow, foreign companies that collect data from U.S. consumers and/or connect to U.S. commercial systems). To date, such measures have generally been considered as one element in proposals to enact a broader Federal privacy law. However, because cybersecurity mandates enjoy more widespread support among stakeholders than a privacy law, Congress should consider passing a standalone cybersecurity law.

Given the vast range of companies that such a law could and should cover, the law should be flexible and process-based. However, to provide appropriate incentives and deterrence, it should empower both the Federal Trade Commission (FTC) and the State Attorneys General to enforce it, and should authorize civil penalties for violations. In addition, to ensure a level playing field across the economy, the law also should cover non-profits and common carriers.

Short of Congress passing such a law, there are a variety of recent and ongoing measures that should be strengthened. First, the FTC should ramp up its efforts to enforce existing privacy laws against companies that fail to implement reasonable security for consumer data, and to educate consumers and business about this important issue. The \$500,000 million allocated to the FTC in the Build Back Better Bill should assist the FTC enormously in this regard.

Second, while I believe the likely success of FTC rulemaking under its Section 5 (Magnuson-Moss) authority has been vastly overstated in some quarters, use of this authority holds promise when it comes to the issue of cybersecurity, and should be considered.

Finally, the Department of Homeland Security has ongoing efforts to engage with the *private sector* to strengthen cybersecurity, and the Administration (pursuant to the recent *executive order*) is attempting to remove barriers to sharing threat information while also imposing strong

cybersecurity measures on companies that contract with the government. Congress should support these important efforts in any way that it can.

Please let me know if I can provide further assistance to you, your staff, or the Committee regarding issues related to cybersecurity and/or privacy more generally.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROGER WICKER TO
JESSICA L. RICH

Question. Today, all 50 states have enacted data breach notification laws. At least 25 states have laws that address the data security of private sector entities. Please answer the following:

Which state (or states) has the strongest breach notification law? Which state (or states) has the least effective breach notification law?

Why is it considered the strongest law? The least effective? Please explain and reference particular elements or features of the law.

Which state (or states) has the strongest data security law? Which state (or states) has the least effective data security law?

Why is it considered the strongest law? The least effective? Please explain and reference particular elements or features of the law.

Of the states identified above, which states have had the most success in preventing cyber incidents and/or responding to security breaches with respect to limiting consumers' exposure to threats and reducing security risks to consumers' data?

Answer. I have not personally conducted a detailed analysis of the relative strength and effectiveness of the many state breach notification and data security laws currently in effect. Also, I think that the effectiveness of each law will largely

depend on how it is enforced. However, as said in my testimony, I do have thoughts about what elements would be desirable in a Federal data security law.

First, it should be process-based so as not to become obsolete when technology changes. At the same time, it should provide enough detail so that it provides sufficient guidance and is enforceable. The standard in the December 2019 proposal from *Privacy for America* (which I helped to draft) provides a good starting point.

Second, the law should cover data security but not breach notification. With state breach notification laws now in effect in all 50 states, I believe including this issue in the law would be highly disruptive to the goals of passing Federal data security legislation.

Third, it should authorize civil penalties to ensure appropriate deterrence. Currently, as you know, the FTC cannot obtain civil penalties for first-time violations.

Fourth, to ensure a level playing field, the law should plug existing holes in the FTC's jurisdiction—notably as to non-profits and common carriers.

Fifth, to achieve consistency while maintaining the important role of the states, it should preempt inconsistent state laws but empower the states to enforce the new law.

Finally, so that the law keeps pace with technological developments, it could provide narrow rulemaking authority (*e.g.*, for issues such as scope of data covered by the rule) coupled with a requirement that the FTC issue periodic guidance regarding specific types of safeguards that could assist with compliance.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
JESSICA L. RICH

Question 1. Do you believe a national standard would benefit both consumers and businesses rather than a patchwork of state laws?

Answer. Yes, a national standard would provide greater clarity to businesses as to their obligations and to consumers as to their rights. It would also provide a mandate and clear direction to the agency(ies) charged with enforcing the law.

Question 2. You mentioned that a private right of action should not be necessary in a Federal data security law. Can you speak to that further?

Answer. One of the main arguments in support of a private right of action is that the FTC, with its limited resources, cannot police the marketplace adequately to promote compliance, deter wrongdoers, and obtain recourse for injured consumers. A strong Federal law could address these concerns by giving the FTC the legal tools and resource it needs, empowering the states to enforce the Federal law, and including strong remedies for violations.

Question 3. What can Congress do to make compliance with a new Federal law less complex, while still ensuring that companies are protecting consumers' data and privacy?

Answer. Passing a strong Federal law establishing a national standard would go a long way towards reducing complexity. The law could preempt inconsistent state laws while giving the states the ability to enforce it—thus achieving consistency while enlisting and empowering the states in the outcome. As noted above, if the law is strong enough, a private right of action should not be necessary.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO
EDWARD W. FELTEN

Protecting Against Ransomware Attacks. Each day, there are over 4,000 ransomware attacks. Recent ransomware attacks such as the attack on the Colonial Pipeline—which halted the distribution of nearly half of the fuel to the East Coast in May—highlight the need to improve the cybersecurity of our critical infrastructure.

Question 1. In 2020, ransomware attacks cost local and state economies over \$18 billion. What do you believe are the greatest current cybersecurity threats to state and local governments?

Answer. Ransomware is among the most important cybersecurity threats faced by state and local governments. These days, everyone faces ransomware threats, but state and local governments may be at particular risk because of the breadth of their missions, the sensitivity of some of their information, and the importance of their work for the people they serve.

Also significant are threats against elections and the operation of democratic processes more generally. These are especially challenging because the existence of

threats can itself undermine confidence and legitimacy of governments, even without any attack, by serving as a subject for disinformation campaigns.

Question 2. What should Congress do to support state and local governments on this issue?

Answer. There are several things Congress can do.

First, Congress can ensure that Federal agencies are vigorously enforcing the law, and are taking action, consistent with Constitutional and statutory limits, to deter and disrupt ransomware networks. These missions are unique to the Federal Government and can make ransomware activities riskier and less lucrative for bad actors.

Second, Congress can ensure that agencies share threat information with state and local governments to the extent possible. This includes assuring that agencies provide necessary help to state and local governments so that their personnel can be appropriately cleared and can set up the systems and processes needed to securely handle sensitive information.

Third, Congress can ensure that Federal agencies make available technical assistance, including information about staffing and best practices. Congress can encourage state and local governments, and organizations representing state and local officials, to work together to develop tools and guidance usable by state and local governments of all sizes.

Fourth, Congress can ensure that when funding is provided through Federal agencies for state and local programs, the funded programs are appropriately required to, and funded for, necessary cybersecurity operations as an integral part of program management.

Question 3. What are the most important actions for Congress to take to stop ransomware attacks on critical infrastructure?

Answer. First, many of the same strategies listed above to help state and local governments will also benefit critical infrastructure providers. Deterrence and threat intelligence are especially important when the potential threat actors are foreign governments, organized crime, or terrorist organizations, which is more likely in the critical infrastructure space. Coordination is also more practical because most critical infrastructure sectors have strong sectoral institutions to support security and preparedness, which can partner with the Federal government.

Second, the impact of ransomware can be reduced by making these infrastructures more resilient overall so that an attack that disables one component or organization causes less harm. This not only reduces the impact of attacks if they do occur; it also decreases adversaries' motive to attack.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KYRSTEN SINEMA TO
KATE TUMMARELLO

State Privacy Laws. Like many states, the Arizona state legislature has considered implementing a consumer privacy law. Three states—California, Colorado, and Virginia—have enacted their own privacy legislation.

Question 1. Do you believe Congress should enact a national consumer privacy law? If so, what are the key elements of a Federal data privacy law to protect Arizonans, especially in regards to data security?

Answer. Engine supports Congress crafting a Federal privacy and data security framework that builds off of the protections in existing state laws but creates one clear, consistent Federal standard, including basic rights around data access and deletion. A Federal framework should also incentivize cybersecurity best practices, such as data minimization and encryption, by protecting organizations for compliance and legal costs if they suffer a data breach despite following best practices.

Question 2. How should a Federal data privacy law interact with state data privacy laws?

Answer. Startups on bootstrap budgets need clarity and consistency. A Federal data privacy and security law should preempt general state data privacy laws, creating one—not a 51st—standard for startups to meet.

FTC Resources. Unfortunately, Arizona schools, hospitals, and companies have been the victims of cyberattacks that have resulted in the release of personal information. Since 2005, data breaches have cost Arizonans at least \$1.6 billion.

Question 1. Considering the costs of these cyber incidents to Arizona and the Nation as a whole, what are your thoughts on providing additional resources to the Federal Trade Commission (FTC) to enforce existing Federal data privacy laws?

Answer. Engine supports the FTC having the resources it needs to enforce existing Federal data privacy laws as well as a potential Federal comprehensive data privacy and security framework.

Question 2. If you believe that additional funding is warranted, what is the appropriate amount of additional funding for FTC enforcement? Should that number be based on whether Congress passes legislation related to data privacy or data security?

Answer. Engine defers to agency experts on whether or how much additional funding is needed for FTC enforcement of current and potential privacy and data security laws, but we encourage Congress to pass a comprehensive Federal privacy and data security framework and equip the FTC with the resources it needs to provide guidance and enforcement for that framework.

Question 3. If a data breach involving their systems occurs, what types of services should companies provide to their consumers?

Answer. The obligations on a company following a data breach should depend on the type and amount of data that was accessed during the breach. If a company holding, for instance, only e-mail addresses suffers a breach, the measures necessary to mitigate the impact on consumers will be different than if a company holding credit card information had suffered a breach.

Compliance Costs. Some tech companies have the resources to employ large numbers of compliance staff to ensure they are following national and state regulations. Many Arizona small businesses do not have access to comparable resources.

Question. How can we craft a Federal data privacy law that does not put small businesses at a disadvantage while still offering consumers strong data security protections?

Answer. Startups and other small businesses need clarity and consistency, including around what kind of data security measures are considered adequate under the law. And, recognizing that even the most responsible companies can fall victim to bad actors, startups need clarity around what steps are required and when they are required to take those steps in the event of a data breach. In addition to the clarity and consistency that a Federal data privacy and security framework can create, the obligations and responsibilities created by the framework regarding data security should depend on several factors, including the amount and type of consumer data a company holds as well as the company's size and resources to shoulder compliance burdens.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RAPHAEL WARNOCK TO
KATE TUMMARELLO

Cybersecurity Workforce Development. Data security is important for both our economic and national security. Just last year, Congress directed the Department of Defense to assess cybersecurity threats to the defense industrial base and the ability of the Department's industrial base and private sector partners to meet software development needs for our national security. I recently visited Project Synergy in Warner Robins, Georgia, a cutting-edge software laboratory built on a partnership between Robins Air Force Base's software depot maintenance and Mercer College's engineering and computer science schools. One of their top requests was increased investment in cybersecurity education and a strong workforce pipeline to ensure they can grow to meet their current needs and the threats of the future.

Question. What is the role of increasing STEM and cyber education in promoting a skilled cybersecurity workforce?

Answer. It is imperative that policymakers support efforts to expand and diversify the country's cybersecurity workforce. As discussed in my testimony, the current cybersecurity talent pool needs an increase both in terms of size and in terms of representation; a large, well-trained, diverse cybersecurity workforce will find and solve more problems in ways that work for more communities of users. Policymakers should expand access to STEM and cybersecurity education across the board—including at varying levels of education—with a focus on increasing access to education and resources in historically underrepresented communities. In comments to the Patent and Trademark Office earlier this year (relevant section attached), Engine examined several facets of this issue as well as potential policy solutions.¹

¹Matt O. Dhaiti, Jamie Dohopolski, and Phillip R. Malone, Engine's Response to the Call for Comments on Expanding American Innovation, Engine (Feb. 23, 2021), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60366ecbd288114c62743c45/1614180046522/Engine+USPTO+diversity+comments.pdf>

Small Business and Economic Development. Businesses of all sizes face threats to their data security, but smaller businesses often have to take on these bad actors with a fraction of the resources as their larger competitors. For example, in my conversations with Georgia's Manufacturing Extension Partnership, I've heard that cybersecurity is one of the top concerns of small manufacturers, and they need more support to understand and implement best practices.

Question 1. How can Congress help small businesses, who may have limited financial and technical resources, keep up with best practices and defend themselves against cybersecurity threats?

Answer. The cybersecurity threat landscape is constantly evolving; deep-pocketed, multinational corporations and government bodies aren't able to defend themselves against all cybersecurity threats. Formal information sharing about specific threats as well as general best practices—including through regularly updated FTC guidance issued as part of a comprehensive Federal privacy and data security framework—would help create a menu of options for startups to consider as they look to protect themselves and their users against cybersecurity threats.

Question 2. How can Congress and the FTC ensure that any new laws and regulations work for businesses of all sizes?

Answer. Startups and other small businesses, by and large, want to be responsible stewards of their users' data. Policy can provide them with clear, consistent guidance around what it takes to be responsible. In this context, Congress should provide a framework that clearly lays out what data security measures are required under the law and what steps are required—and when they are required—in the event of a data breach. If the FTC is granted rulemaking authority under a Federal privacy and data security law, the agency should ensure that obligations and responsibilities scale based on the amount and type of consumer data a company holds as well as the company's size and resources to shoulder compliance burdens.

EDUCATION & TRAINING

While improving access to capital and expanding networks for underrepresented entrepreneurs may yield more near-term results, federal entities should also improve education opportunities for underrepresented innovators so that they are equitable and inclusive, affecting long-lasting change. This includes improving access to science, technology, engineering, and mathematics (STEM) education, but it also applies to business and innovation and entrepreneurship (I&E) education and training for underrepresented students. Greater access and retention is critical because the nation needs diverse students in the talent pipeline. In order to achieve that goal, diversity of STEM, business, and I&E educators is also critical but often overlooked.

Diversity gaps among students and educators.

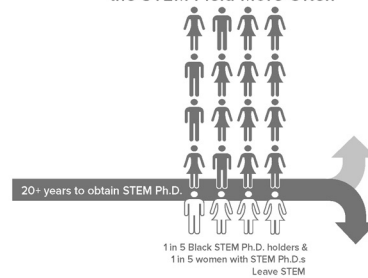
Retention of Students in Innovation Careers

The nation's innovation ecosystems need high-skilled, diverse talent. In order to grow and sustain diversity in innovation, the government should invest in a diverse talent pipeline because, beyond funding, building a team is one of the biggest challenges facing startups. A successful talent pipeline not only starts early to excite young students about innovation, but it also requires encouraging talented students to channel that excitement into innovation careers.

Disparities in education representation are compounded by problems of retention, which cuts off the innovation pipeline too early for students who cannot or do not want to pursue innovation careers. Students of color represent 38.5 percent of STEM postsecondary students,¹⁴⁷ but Black and Latino students switch out of STEM degree programs at higher rates than their white peers.¹⁴⁸ In addition, an estimated 20 percent of Black STEM

Ph.D. holders and 20 percent of women STEM Ph.D. holders leave STEM fields.¹⁴⁹ And the retention problems only continue, creating further underrepresentation in the workplace: of all STEM professionals, only 9 percent are Black and only 7 percent are Latino.¹⁵⁰

Women and Black Ph.D. Holders Leave the STEM Field More Often



Beyond a lack of representation in STEM fields, taking a closer view—and acknowledging that not all STEM jobs are created equal—reveals other relevant disparities across STEM fields. For example, computer jobs feature one of highest median earnings of any STEM field, but the computer workforce is only 14 percent Black or Latino and only 25 percent women.¹⁵¹ On the other end of the salary median are healthcare practitioners and technicians.¹⁵² And it is these lower paying fields that have the highest representation of Black, Latino, and women workers. By way of example, 37 percent of licensed nurses are Black or Latino as are about a quarter of health support, medical record, and clinical laboratory technicians.¹⁵³ Women, on the other hand, comprise 75 percent of healthcare practitioners and technicians.¹⁵⁴

¹⁴⁷ Nat'l Ctr. For Educ. Stat., *Table 318.45, Dig. Educ. Stat.* (Oct. 2019), https://nces.ed.gov/ipeds/data/digest/tables/dt19_318.45.asp (2017-2018 percentages).

¹⁴⁸ Emily Arnum, *A Third of Minority Students Leave STEM Majors*.

Here's Why, EAB (Oct. 8, 2019), <https://eab.com/insights/daily-briefing/student-success/a-third-of-minority-students-leave-stem-majors-heres-why/>; see also Univ. of Ill. Coll. of Agric., Consumer & Env't Scis., *Racial Microaggressions Contribute to Disparities in STEM Education*, ScienceDaily (Dec. 8, 2020), <https://www.sciencedaily.com/releases/2020/12/201208111636.htm>.

¹⁴⁹ See Carol O'Donnell & Shelina Ramnarine, *An Integrated Approach to Diversity, Equity, Accessibility and Inclusion (DEAI) in STEM*, Smithsonian Sci. & Educ. Ctr. (2019), available at <https://ssecc.si.edu/sites/default/files/other/STEMLeadershipAlliance2020.pdf>.

¹⁵⁰ Cary Funk & Kim Parker, *Women and Men in STEM Often at Odds Over Workplace Equity*, Pew Rsch. Ctr. 8 (Jan. 9, 2018), https://www.pewresearch.org/social-trends/wp-content/uploads/sites/3/2018/01/PS_2018.01.09_STEM_FINAL.pdf.

¹⁵¹ *Id.* at 16, 34, 36.

¹⁵² *Id.*

¹⁵³ *Id.* at 34.

¹⁵⁴ *Id.* at 30.

EDUCATION & TRAINING

Understanding STEM's "leaky pipeline," and ensuring that underrepresented innovators are inspired and able to pursue lucrative careers, will require further data collection; and Engine encourages NCEAI to call for that. But anecdotal evidence suggests that disparate access to education, lack of encouragement at an early age, discrimination, difficulty balancing work and family, and lack of representation are barriers to entering STEM jobs for underrepresented innovators of color and women innovators.¹⁵⁵

It is also important to note that fostering STEM jobs should be inclusive of those positions that do not require postsecondary education. Innovation does not require a degree, so inquiry into innovation retention should not focus on only advanced education-related factors. For example, alternative education like immersion programs or "boot camps" can be another successful path to STEM and innovation careers.¹⁵⁶

Finally, in addressing retention, geography is another important factor: innovation industries, talent, and jobs cluster in a few cities.¹⁵⁷ And rural communities that may be successful at turning out students interested in STEM tend to lose talent to other regions upon graduation. Indeed, some entrepreneurs looking to launch companies outside those traditional tech sectors face pressure to relocate so that they can connect with investors and talent.¹⁵⁸

Startup Testimonial:

*On Missoula's startup ecosystem: "Our number one challenge right now is continuing to fuel the talent pipeline. When I first moved here, Montana's biggest export was its talent, we used to lose a lot of people to big cities and traditional hubs. What we're going through now is trying to help the students coming through our universities understand that there are great career opportunities here. We are also trying to get the word out to Montanans who have left here and want to come back that the opportunities with successful companies exist."*¹⁵⁹

¹⁵⁵ *Id.* at 21.

¹⁵⁶ For a discussion of some alternative pathways to STEM education and STEM careers, see Joe Alper, *Developing a National STEM Workforce Strategy: A Workshop Summary*, Nat'l Acad. 63-70 (2016), available at <https://www.nap.edu/read/21900/chapter/8>.

¹⁵⁷ Eduardo Porter, *A Few Cities Have Commanded Innovation Jobs. Can That Be Changed?*, N.Y. Times (Dec. 9, 2019), <https://www.nytimes.com/2019/12/09/business/economy/innovation-jobs-cities.html>.

¹⁵⁸ Nathan Lindfors, *Cultivating a Marketplace for Farmers Using Technology*, Engine (Nov. 24, 2020), <https://www.engine.is/news/startupseverywhere-midhattan-kan-hitchpin> (interviewing Trevor McKeeman, CEO of Hitchpin in Kansas).

¹⁵⁹ Andrew Jones, *#StartupsEverywhere: Missoula, MT*, Engine (Mar. 26, 2018), <https://www.engine.is/news/category/startupseverywhere>.

Startup Testimonial:

*On Effingham's startup ecosystem: "[T]he hardest part about staying in a rural community, especially when you leave high school and go to college, is not understanding or knowing what the local opportunities are. It would be great to have a program funded by the government, at the high school level, that allows local companies to engage with students. For students at Effingham High School, it would be great to educate them about the local job opportunities as part of career development. If students going from high school to college don't know about their local opportunities or companies, then they won't come back because they don't know that there are good jobs for them in rural communities."*¹⁶⁰

Innovation Educators

To better encourage and foster diversity in innovation, the government should invest in underrepresented STEM and business educators as well as students.

The diversity of educators matters because representation matters.¹⁶¹ The opportunity for students to identify themselves in their educators instills the belief in students that they, too,

missoula-mt (interviewing Paul Gladen, director of Blackstone Launchpad at the University of Montana).

¹⁶⁰ Edward Graham, *Streamlining Across Reporting Solutions for Farmers*, Engine (Aug. 28, 2020), <https://www.engine.is/news/startupseverywhere-effingham-ill-myagdata> (quoting Deb Casarella, co-founder and CEO of MyAgData in Illinois).

¹⁶¹ The same is true in fields other than education. Lack of representation leads to additional inequalities and exacerbates existing ones. This is well-documented in medicine, where Black patients face more adverse outcomes when treated by white doctors than when treated by Black doctors. See, e.g., Erin Dehon et al., *A Systematic Review of the Impact of Physician Racial Bias on Clinical Decision Making*, 24 Acad. Emergency Med. 895 (2017); Nat'l Acad., *Unequal Treatment: Confronting Racial and Ethnic Disparities in Health Care* 3-12, 19 (Brian D. Smedley, Adrienne Y. Smith, & Alan R. Nelson eds., 2003); see also Talia Milgrom-Ekott, *Students of Color Are Missing Out on STEM Opportunities. So the Planet Is Missing Out on Their Brilliance. Here's How We Finally Achieve Equity in High School STEM*, Forbes (Sept. 24, 2020), <https://www.forbes.com/sites/taliamilgromekott/2020/09/24/students-of-color-are-missing-out-on-their-brilliance-heres-how-we-finally-achieve-equity-in-high-school-stem/?sh=52eba28e5148> (making the connection between the effects of representation in medicine and in education).

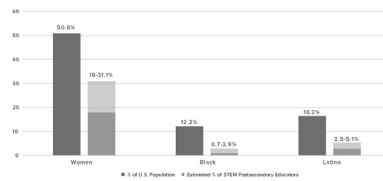
EDUCATION & TRAINING

belong as innovators.¹⁶² This is due, at least in part, to role model effects and cultural understanding. Diverse educators serve as role models and signal to underrepresented students that they have a future in STEM, innovation, and entrepreneurship.¹⁶³ Additionally, cultural understanding between educators and students helps ensure that material is explained in a “culturally relevant and engaging way.”¹⁶⁴ As one expert describes the effects, “[a] diverse staff allows more students to see themselves in their teachers, school leaders, and other school personnel. . . . [and] provides more opportunities for students to find someone they can connect with, whether through shared culture or other experiences.”¹⁶⁵

Representation in education is essential because it encourages more underrepresented students to choose a career of innovation and entrepreneurship. Early exposure to inclusive innovation education excites and motivates students to pursue STEM, business, and innovation higher education, and from there, careers. As Irma Olguin Jr., co-founder and co-CEO of Bitwise, explains, joining an innovation ecosystem “shouldn’t be an unfathomable option[] or an accident for anyone.”¹⁶⁶

Unfortunately, the educator workforce is less diverse than the population. STEM and business education begins far earlier than college,¹⁶⁷ so the government should start by looking at educators

Underrepresented Groups in STEM Education, Compared to Representation in U.S. Population



in primary and secondary schools, where a recent report by the Department of Education found that only 18 percent of educators were people of color,¹⁶⁸ while over the same time, 36 percent of the population identified as people of color.¹⁶⁹

The same is true for postsecondary educators. Only 24 percent of university faculty members in the U.S. are people of color.¹⁷⁰ And across STEM fields, the statistics are even bleaker. According to a 2017 study, 12.2 percent of the population is Black, but only 0.7 to 2.9 percent of STEM faculty are Black.¹⁷¹ And while 16.3 percent of the population is Latino, between 2.5 to 5.1 percent of postsecondary STEM faculty identify as such.¹⁷² Gender parity is likewise absent, with only 18 to 31.1 percent STEM postsecondary educators identifying as women despite comprising 50.8 percent of the population.¹⁷³

¹⁶² See Christopher Redding, *A Teacher Like Me: A Review of the Effect of Student-Teacher Racial/Ethnic Matching on Teacher Perceptions of Students and Student Academic and Behavioral Outcomes*, 89 Rev. Educ. Res. 499 (2019).
¹⁶³ See Seth Gershenson et al., *The Long-Run Impacts of Same-Race Teachers*, Nat'l Bureau Econ. Res. (Nov. 2018), available at <https://www.nber.org/papers/w25254>.

¹⁶⁴ See Anna J. Egalite & Brian Kisida, *The Effects of Teacher Match on Students' Academic Perceptions and Attitudes*, 40 Educ. Evaluation & Policy Analysis 59, 75 (2018); see also *Cultivating Native American Entrepreneurship in Northern Michigan*, Engine (Jan. 29, 2021), <https://www.engine.is/news/startupseverywhere-traverse-city-nich-arrowhead-incubator> (interviewing Shaloh Slomsky, executive director and co-founder of Arrowhead Incubator in Michigan, and describing the power of infusing culture into business training for Native American entrepreneurs, like by lecturing in traditional attire).

¹⁶⁵ Daniel A. Domenech, *How Is Why Diversity in STEM Education Is So Important*, Educ. & Career News, <https://www.educationandcareersnews.com/education-technology/here-is-why-diversity-in-stem-education-is-so-important/> (last visited Feb. 9, 2021) (interviewing and quoting Kendell V. Ali).

¹⁶⁶ Bitwise, *supra* note 127.

¹⁶⁷ See Edward Graham, *Using Technology to Support Child Care Providers*, Engine (Oct. 4, 2019) <https://www.engine.is/news/startupseverywhere-pittsburgh-pa> (interviewing Shaina Williams, co-founder of C.C. Busy in Pennsylvania, who discusses the need to start STEM education as

early as preschool); Andrew Jones, *#StartupEverywhere: Kansas City, MO*, Engine (May 15, 2018), <https://www.engine.is/news/category/startupseverywhere-kansas-city-mo?q=Missouri> (interviewing Ryan Weber, president of the KC Tech Council in Missouri, who notes the disparity in computer science education across schools in Missouri).

¹⁶⁸ U.S. Dep't of Educ., *The State of Racial Diversity in the Educator Workforce at 3, 6* (July 2016), available at <https://www2.ed.gov/rschstat/eval/highered/racial-diversity/state-racial-diversity-workforce.pdf>.

¹⁶⁹ Stephanie Ewart, *U.S. Population Trends: 2000 to 2060*, U.S. Census Bureau at 7 (Oct. 15, 2015), available at <https://www.ncsl.org/Portals/1/Documents/nalfo/USDemographics.pdf>.

¹⁷⁰ Leslie Davis & Richard Fry, *College Faculty Have Become More Racially and Ethnically Diverse, But Remain Far Less So Than Students*, Pew Res. Ctr. (July 31, 2019), <https://www.pewresearch.org/fact-tank/2019/07/31/us-college-faculty-student-diversity/>.

¹⁷¹ Diyi Li & Cory Koedel, *Representation and Salary Gaps by Race-Ethnicity and Gender at Selective Public Universities*, 46 Educ. Researcher 343, 346, 347 tbl.3 (2017). Note that the Li and Koedel used the 2010 census demographic data in making their comparisons. Demographic data from the 2020 census remains outstanding, but it is expected that the proportion of nonwhite residents has only grown, meaning these data underestimate the disparity in representation.

¹⁷² *Id.*
¹⁷³ *Id.*

EDUCATION & TRAINING

Funding STEM and I&E education initiatives for underrepresented students and educators.

To diversify American innovation ecosystems, the government should invest in local and federal programs aimed at improving access to STEM and I&E teaching and education across primary, secondary, and postsecondary levels.

Improving and Expanding Programs for Students.

Access to STEM and I&E education should improve on two axes. First, the government should ensure innovation education resources and programs are available to underrepresented students regardless of race, gender, or geography. This includes access to STEM and I&E educators as well as to innovation and entrepreneurial co-curricular and extracurricular activities. Second, those resources should be presented in ways that are tailored to and engaging for underrepresented students.

Startup Testimonial:

"I worked on a bill to provide funding to STEM organizations that focus on students of color across Georgia's education system. That funding has gone to create STEM clubs across the state. We are hosting targeted workshops, and we are seeing more Black and Latino children engaged with science and math throughout the course of their education. I wanted to be part of this effort to give students opportunities that I did not have at their age. If I had a STEM club in elementary school, then I think I would have been an aerospace engineer a lot earlier in my career."¹⁷⁴

The federal government should invest in programs aimed at expanding and revising STEM and I&E curriculum resources so that innovation education is exciting and inviting to all students. Federal entities can fund and encourage state and local funding of tailored education programs for

students of all ages—from early childhood to postgraduate education—and highlight contributions of diverse innovators. Additionally, the government should invest in local STEM and I&E co-curricular and extracurricular programs for primary and secondary schools in underserved communities.¹⁷⁵ For postsecondary education, the government should invest in innovation-related clubs at HBCUs, land-grant universities, and other postsecondary education institutions that attract more diverse student bodies, including community colleges.

It is also vital that innovation educators establish inclusive environments.¹⁷⁶ Doing so requires that educators reflect on their own identities and privileges, recognize the multidimensional motivations and aspirations of their students, and highlight STEM and I&E contributions by diverse entrepreneurs.¹⁷⁷ Instead of focusing on only Thomas Edison, for example, the works of Percy Julian, Sarah Boone, and Katharine Burr Blodgett also should be center stage.

Increasing Diversity Among Educators.

The government should encourage and invest in efforts to diversify the educator workforce. For example, alternative-route certification programs attract more diverse educators and should be expanded.¹⁷⁸ The government should also increase funding for initiatives like the Smithsonian STEM Education Summit and 100Kin10 that specifically seek to increase diversity in STEM and I&E education.¹⁷⁹ More broadly, the government should build and encourage the narrative that teaching STEM is a viable career path for all, both through explicit programming and through more expansive loan forgiveness.

The government should also take an active role in reaching out to and connecting with potential underrepresented educators.

¹⁷⁵ See, e.g., *Project Invent Fellowship*, Project Invent, <https://projectinvent.org/for-educators> (last visited Jan. 29, 2021); Graham, *Infiltron*, *supra* note 12 (discussing STEM program focusing on students of color across Georgia).

¹⁷⁶ Alison Singer, Georgina Montgomery, & Shannon Schmoll, *How to Foster the Formation of STEM Identity: Studying Diversity in an Authentic Learning Environment*, *Inf'11 STEM Educ.* (Nov. 6, 2020), <https://doi.org/10.1186/s40594-020-00254-z>.

¹⁷⁷ See Tess L. Killpack & Laverne C. Melón, *Toward Inclusive STEM Classrooms: What Personal Role Do Faculty Play?*, *CBE Life Sci. Educ.* (Oct. 13, 2017), <https://www.lifescied.org/doi/full/10.1187/cbe.16-01-0020>.

¹⁷⁸ U.S. Dep't of Educ., *supra* note 168, at 17.

¹⁷⁹ *STEM Education Summit: Building a Coalition for Attracting and Retaining a Diverse STEM Teaching Workforce*, Smithsonian Sci. & Educ. Ctr., <https://ssec.si.edu/event/stem-education-summit-building-coalition-attracting-and-retaining-diverse-stem-teaching> (last visited Jan. 28, 2020); *Our Story*, 100Kin10, <https://100kin10.org/about> (last visited Jan. 28, 2021).

¹⁷⁴ Graham, *Infiltron*, *supra* note 12 (quoting Chastity Wright of Infiltron).

EDUCATION & TRAINING

For example, the Department of Education should actively recruit underrepresented educators to join the STEM and I&E education workforce. Action produces results: as Washington University in St. Louis demonstrated with its practice of solicitation and invitation for its Women in Innovation and Technology program, actively reaching out to underrepresented educators diversifies the innovation educator workforce which in turn provides role models for underrepresented students to see themselves in STEM and I&E.¹⁸⁰

Investing in I&E Education Programs Focused on Underrepresented Innovators.

The government should also look to I&E education as a path to expand American innovation. Innovation and entrepreneurship are often complex and non-linear, and preparing students to succeed requires different educational approaches compared to traditional disciplines.¹⁸¹ Exstant I&E programs range from guiding students from an idea to a business or technology launch to focusing further upstream by training students to be more innovative and creative.¹⁸² Indeed, I&E are core skills, and training students to be more innovative should be considered a part of the core curriculum from a young age.¹⁸³

Because I&E programs are often interdisciplinary, attracting

students from across an institution, they can create a natural pull towards diversity. Well-designed I&E programs can encompass students from a broad range of disciplines—engineering, computer science, psychology, sociology, marketing, finance, law, nursing, and more. And in so doing, I&E programs can attract students who may shy away from traditional STEM fields but are interested in learning about innovation.¹⁸⁴

Many I&E programs currently look to private donors¹⁸⁵ and may struggle to compete for traditional government funding because they do not fit tidy STEM definitions. While these private donations add a lot of value, I&E programs reliant on private funds are often targeted to the donor's particular interests and can be difficult to scale. The government should consider establishing dedicated funding pools or issuing specific grant opportunities for I&E education. This would make it easier to expand U.S. innovation and would enable schools that lack a wealthy donor base to launch successful I&E programs. The government could also expand existing programs like NSF's I-CORPS, which is designed to support the commercialization of new technologies and reduce the risk and time required to translate new ideas to the market.¹⁸⁶

Importantly, the government should also identify gaps in diversity for its current I&E investments and develop new, dedicated programs that serve all underrepresented students. Existing I&E education investments provide a start, but they do not fully accomplish this goal. For example, while I-CORPS has made strides broadening participation by women,¹⁸⁷ participation by other underrepresented groups is still lacking.¹⁸⁸ The government should consider establishing additional programs at institutions that attract a more diverse student body, like HBCUs, land-grant universities, and community colleges.

¹⁸⁴ Indeed, the student population of certain I&E programs mirrors the diversity of the entire student population. *Compare, e.g.,* Duke Univ., *Scaling, Duke Innovation & Entrepreneurship*, <https://entrepreneurship.duke.edu/> at 2019-2020 scaling/ (last visited Feb. 18, 2021) with Duke Facts, <https://facts.duke.edu/> (last visited Feb. 22, 2021) (I&E students drawn from multiple majors across the university, where the demographic data of the I&E program are highly similar to that of the overall university).

¹⁸⁵ *See, e.g.,* A. James & Alice B. Clark Found., *A. James Clark Scholars Program*, <https://clarkfoundationdc.org/clark-scholars/> (last visited Feb. 11, 2021).

¹⁸⁶ Nat'l Sci. Found., *National Science Foundation Innovation Corps*, https://www.nsf.gov/news/special_reports/i-corps/about.jsp (last visited Feb. 12, 2021).

¹⁸⁷ Nat'l Sci. Found., *Innovation Corps (I-Corps): Biennial Report 13* (Spring 2019), https://www.nsf.gov/news/special_reports/i-corps/pdf/I-CorpsReport-6_4_19FINAL_508.pdf.

¹⁸⁸ *See id.* at 26 (noting that, of 1626 individuals, only 453 were from underrepresented groups but 338 of those were women and reporting that only 208 team leads were from underrepresented groups but 164 of those were women); Nat'l Sci. Found., *A National Initiative to Develop Diversity and Inclusion Infrastructure for STEM Innovation*, https://www.nsf.gov/awardsearch/showAward?AWD_ID=1940055 (last visited Feb. 11, 2021).

¹⁸⁰ Wash. Univ. in St. Louis, Comment Letter on Request for Comments on the SUCCESS Act of 2018, at 2-3 (June 27, 2019), <https://www.uspto.gov/sites/default/files/documents/SUCCESSAct-Washington-University-in-St-Louis.pdf>.

¹⁸¹ *See* Gabriel Linton & Markus Klinton, *University Entrepreneurship Education: A Design Thinking Approach to Learning, J. Innovation & Entrepreneurship* (Jan. 14, 2019), <https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-018-0098-z>.

¹⁸² *See* Martin Läckens, *Entrepreneurship in Education: What, Why, When, How*, *Entrepreneurship360*, at 1 (2015), https://www.oecd.org/cfe/leed/BGP_Entrepreneurship-in-Education.pdf (noting that the definition of entrepreneurship can vary, from training students to start a business to making students more creative). For examples of I&E programs, *see* Duke Univ., *Education*, Duke Innovation & Entrepreneurship, <https://entrepreneurship.duke.edu/education/> (last visited Feb. 12, 2021); Ga. Inst. of Tech., *TIGER Program*, Ga. Tech Scheller Coll. Bus., <https://www.scheller.gatech.edu/centers-initiatives/tiger/index.html> (last visited Feb. 12, 2021); and Univ. Colo. Colo. Springs, *UCCS Bachelor of Innovation*, <https://innovation.uccs.edu/what-is-the-bi/>. *See also* U.S. Dep't of Com., *The Innovative and Entrepreneurial University: Higher Education, Innovation & Entrepreneurship in Focus 10-12* (Oct. 2013), https://www.eda.gov/pdf/The_Innovative_and_Entrepreneurial_University_Report.pdf (listing select programs).

¹⁸³ One model, the Network for Teaching Entrepreneurship (NFTe), is an education non-profit focused on bringing entrepreneurship to middle and high school students, as well as educators, in low-income communities. NFTe, NFTe, <https://www.nfte.com/> (last visited Feb. 18, 2021).



RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROGER WICKER TO
KATE TUMMARELLO

Question. Today, all 50 states have enacted data breach notification laws. At least 25 states have laws that address the data security of private sector entities. Please answer the following:

Which state (or states) has the strongest breach notification law? Which state (or states) has the least effective breach notification law?

Why is it considered the strongest law? The least effective? Please explain and reference particular elements or features of the law.

Answer. It's difficult to pin down the strongest or least effective state data breach notification law, as laws have multiple provisions, each of which could be considered stronger or less effective. But some state data breach notification laws contain provisions that are particularly strong or ineffective and should be informative for policymakers crafting a Federal privacy and data security law with an eye towards the clarity and consistency that startups need.

While startups recognize the need to protect their users' data, some amount of data breaches are inevitable as the landscape of cybersecurity threats is vast and evolving. Some state laws have provisions that minimize compliance uncertainty when an organization has been breached, which helps ease the burden for startups that are already grappling with a costly and time-consuming breach. For instance, California law provides a template data breach notification letter, which clearly spells out what information must be included in notification for a company to be in compliance with the law if they've suffered a data breach and need to notify consumers. State laws that provide means for substitute notice in lieu of individual notification for affected consumers in some circumstances also help ease compliance burdens in the wake of a breach.

But state laws that keep organizations that have suffered a data breach from clearly communicating the fact of the breach and relevant context put organizations, including startups, in the difficult position of having to communicate an incomplete picture to users. Massachusetts prohibits organizations that have suffered a data breach from including in their notice to consumers "the nature of the breach." In addition to conflicting with other state laws that require organizations to include a description of the data breach in notices to consumers, the Massachusetts law risks arming consumers with insufficient information if their data has been compromised in a data breach.

Which state (or states) has the strongest data security law? Which state (or states) has the least effective data security law?

Why is it considered the strongest law? The least effective? Please explain and reference particular elements or features of the law.

Answer. Again, it's difficult to say which state data security law is the strongest and which is the least effective, but policymakers can learn lessons from varying provisions of multiple states' laws about what works well and what doesn't. Effective state data security laws incentivize organizations, including startups, to proactively take steps to secure their users' data without being overly prescriptive or ignoring the reality that different security measures will make sense for different organizations based on their resources and the amount and type of data they hold.

A few states have found ways to incentivize security measures—such as encryption—by easing regulatory and legal burdens if an organization suffers a breach despite using those security measures. As discussed in my written testimony, startups on tight budgets—the average seed-stage startup has about \$55,000 per month to cover all of its costs, and the vast majority of startups have much less—are particularly ill-equipped to spend hundreds of thousands of dollars on litigation. Under the California Consumer Privacy Act, an organization that suffers a data breach is granted immunity from the law's private right of action where the only data obtained in the breach is encrypted. The law's private right of action carries potential statutory damages on top of typical legal costs, so the ability to evade a costly and time consuming lawsuit is a powerful incentive for companies to encrypt users' data. Other states have similar incentives, including the Ohio Data Protection Act, which provides an affirmative defense against certain data breach tort claims if the organization followed cybersecurity best practices. Engine remains concerned about the inclusion of a private right of action in any Federal privacy, data security, and/or data breach notification law, but these kinds of incentives should be included and expanded in a Federal law to mitigate the risk of harm to startups from onerous regulatory or legal action.

One of the less helpful elements of state data security laws is mandates that organizations comply with "reasonable data security measures" without specifying what

that entails. While it's critical that any data security framework be flexible and scalable, a startup needs to know it's in compliance with the law without having to survive a regulatory or legal challenge in the event of a breach. Engine supports FTC rulemaking authority to create a flexible, scalable data security framework that can be regularly updated as technology and the threat landscape evolve, creates clear, consistent standards for startups to meet, and takes into account the resources available to organizations as well as the amount and type of data they hold.

Of the states identified above, which states have had the most success in preventing cyber incidents and/or responding to security breaches with respect to limiting consumers' exposure to threats and reducing security risks to consumers' data?

Answer. Given the inherently interstate nature of the Internet and the flow of data, it's difficult to identify which state has the best record with cyber incidents and data breaches and even more difficult to tell if that record is the direct result of the state's data security and data breach notification laws. However, California's data security and breach notification framework, taken on the whole, is widely considered the original and gold standard, and Congress should especially look at what is working well in that state, including the elements mentioned above.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
KATE TUMMARELLO

Question 1. In your testimony, you mention that the current patchwork of state laws drive up startups' compliance costs without providing any benefits to consumers.

Can you elaborate on the effects a patchwork of state laws have on small businesses, and would a single Federal law be preferable for both businesses and consumers?

Answer. Thank you for the opportunity to elaborate on the burdens the current patchwork of state laws can create for startups. The small and young companies across the country that make up the startup ecosystem overwhelmingly want to do the right thing and protect their users' data. That's one of the many competing pressures startups face as they launch and scale. In fact, many startups compete on privacy and security and use strong security protections as a way to differentiate themselves from their large competitors.

It is, unfortunately, impossible for a startup—or any company, organization, government agency, etc.—to be completely immune to data breaches; the technological capabilities of bad actors and the threat landscape is constantly evolving. Knowing they should be responsible but can't be perfect in preventing data breaches, startups need clarity and consistency around their obligations under data security and data breach notification laws. Currently, startups have to navigate a mosaic of dozens of state laws around data security and 50 state laws around data breach notification. Even where the laws have similar substantive goals, small differences can create compliance costs and burdens that are difficult for startups on bootstrap budgets—the average seed-stage startup has roughly \$55,000 per month to cover all costs, and the vast majority of startups have much less—to navigate. Those burdens increase substantially when the laws explicitly conflict.

A single, Federal law around how companies process and store data and notify users in the event of a data breach would give the startup ecosystem much-needed consistency and clarity. At the same time, a single Federal law could be written to build off of the strongest consumer protections that exist, which would expand stronger protections to all consumers across the country.

It's critical that a Federal law not open the door to a new patchwork of requirements as determined by courts across the country as they rule on private lawsuits brought under a new Federal law. While a private right of action could be narrowly tailored to go after bad actors in clear cut circumstances, a sweeping, unrestrained private right of action would just shift the patchwork from state capitals to court-houses.

Question 2. What can Congress do to make compliance with a new Federal law less complex, while still ensuring that companies are protecting consumers' data and privacy?

Answer. Startups need clear, consistent rules, and they need to know that if they follow the rules, they won't be subject to onerous regulatory and legal costs. On data security, Engine supports giving the FTC rulemaking authority to craft rules that provide a menu of options for startups to choose from based on the resources available to them and the amount and types of data they hold. Congress should include in a law a requirement that the FTC update the rules regularly to keep up with advancing technological capabilities and threats.

More generally, Congress can minimize complexity by preempting the current patchwork of state laws, ensuring enforcement is coordinated—so that what is permitted under the reading of the law in one jurisdiction isn't prohibited in another—and, if Congress includes a private right of action in the law, crafting a narrowly tailored private right of action that doesn't open the door to bad faith litigation or disparate court rulings about what is permissible under the law.

