

PROTECTING CONSUMER PRIVACY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 29, 2021

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



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

U.S. GOVERNMENT PUBLISHING OFFICE

53-124 PDF

WASHINGTON : 2023

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

DAVID STRICKLAND, *Staff Director*

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 September 29, 2021	Page 1
Statement of Senator Cantwell	1
Statement of Senator Wicker	3
Letter dated September 27, 2021 from civil rights, civil liberties, and consumer protection organizations to Hon. Maria Cantwell and Hon. Roger Wicker	6
Letter dated September 28, 2021 from Arthur Sidney, Vice President of Public Policy, Computer & Communications Industry Association to Hon. Maria Cantwell and Hon. Roger Wicker	11
Letter dated September 28, 2021 from the Main Street Privacy Coalition to Hon. Maria Cantwell and Hon. Roger Wicker	15
Letter dated September 28, 2021 from David French, Senior Vice Presi- dent, Government Relations, National Retail Federation to Hon. Maria Cantwell and Hon. Roger Wicker	19
Letter dated September 29, 2021 from Aaron Cooper, Vice President, Global Policy, BSA The Software Alliance to Hon. Maria Cantwell and Hon. Roger Wicker	20
Letter dated September 29, 2021 from Kirsten Gillibrand, United States Senator from New York	23
Article dated September 29, 2021 from <i>The Wall Street Journal</i> entitled, “FTC Weighs New Online Privacy Rules” by John McKinnon and Ryan Tracy	84
Statement of Senator Baldwin	89
Statement of Senator Tester	90
Statement of Senator Fischer	92
Statement of Senator Klobuchar	94
Statement of Senator Scott	95
Statement of Senator Moran	97
Statement of Senator Markey	99
Statement of Senator Thune	100
Statement of Senator Hickenlooper	102
Statement of Senator Lummis	104
Op-Ed dated September 27, 2021 entitled “The bipartisan reason Con- gress should regulate big tech” by Senator Cynthia Lummis	105
Statement of Senator Peters	108
Statement of Senator Lee	110
Statement of Senator Rosen	112
Statement of Senator Warnock	113
Statement of Senator Luján	115
Statement of Senator Blumenthal	117

WITNESSES

David C. Vladeck, Professor and Faculty Director, The Center on Privacy and Technology, Georgetown Law; Former Director, Federal Trade Commis- sion, Bureau of Consumer Protection	26
Prepared statement	27
Maureen K. Ohlhausen, Partner and Section Chair of Antitrust and Competi- tion Law, Baker Botts; Former Acting Chairman, Federal Trade Commis- sion	33
Prepared statement	34
Ashkan Soltani, Independent Researcher and Technologist; Former Chief Technologist, Federal Trade Commission	38
Prepared statement	40
Morgan Reed, President, ACT The App Association	69

IV

	Page
Morgan Reed, President, ACT The App Association—Continued	
Prepared statement	70

APPENDIX

Color of Change, prepared statement	121
Electronic Transactions Association, prepared statement	123
Privacy4Cars, prepared statement	126
Response to written question submitted to David C. Vladeck by:	
Hon. Ray Ben Luján	130
Hon. Raphael Warnock	130
Hon. John Thune	130
Hon. Marsha Blackburn	131
Response to written questions submitted to Maureen K. Ohlhausen by:	
Hon. Ben Ray Luján	131
Hon. Raphael Warnock	131
Hon. John Thune	132
Hon. Marsha Blackburn	132
Response to written questions submitted to Ashkan Soltani by:	
Hon. Ben Ray Luján	133
Hon. Raphael Warnock	133
Response to written questions submitted to Morgan Reed by:	
Hon. Raphael Warnock	135
Hon. John Thune	136
Hon. Marsha Blackburn	137

PROTECTING CONSUMER PRIVACY

WEDNESDAY, SEPTEMBER 29, 2021

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

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

Present: Senators Cantwell [presiding], Klobuchar, Blumenthal, Markey, Peters, Baldwin, Tester, Rosen, Luján, Hickenlooper, Warnock, Wicker, Fischer, Moran, Blackburn, Young, Lee, Scott, and Lummis.

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

The CHAIRWOMAN. The U.S. Committee on Commerce, Science, and Transportation will come to order. Good morning, everyone. Today, we are having a hearing on protecting consumer privacy. And we will hear from a panel of experts, three of whom have previously been on the front lines of fighting to protect consumer privacy at the primary agency charged with protecting consumers' privacy and data security, the Federal Trade Commission.

We all know the challenges of the information age, and that they have brought us new products and services. But it has also exposed and threatened consumer privacy by unnecessarily collecting, storing, selling, and exposing consumers' most personal data to theft and harm. Every year for the past 5 years, more than 140 million people have been affected by data breaches, exposing their personal data to thieves and fraudsters. And from July 2019 through July 2020, more than 650,000 residents of my state, Washington, were victims of data breaches, including the release of their healthcare information, banking records, Social Security numbers, credit card information.

Last week it was reported that Simon—last week it was reported that last May, Simon Eye, a U.S. chain of optometry clinics, had been data breached, exposing 144,000 individuals to sensitive—their sensitive data. This past April, the personal data of over 500 million Facebook users, including phone numbers, full names, locations, e-mail addresses, were posted in a hacking forum, 32 million records were from the United States, providing key information with people who would want to use those in various ways. And last June, Volkswagen announced a data breach and exposed phone numbers and e-mail addresses of 3.1 million Americans who had shopped for cars.

So it isn't a surprise that all this data being stolen, exposed, that more people have become victims of identity theft. Identity theft complaints have increased 375 percent between 2017 and 2020. The harms are causing real damage to consumers. According to a May 2021 report by the Identity Theft Resource Center, victims of identity theft are turned down for loans, unable to rent houses. They have their credit damaged. They are billed for medical services they never received. Can't find unemployment benefits because their name was basically stolen.

Our precise locations, fitness regimens, computer strokes, and even our friends and family networks have basically been turned into commodities. We know that recently *The Wall Street Journal* also found that even after you turn off some of your app tracking on your iPhone, iPhone apps can continue to track you using your device fingerprints. The fact is that companies collecting this information are not doing enough to safeguard and collect—the information that they collect or keep their privacy promises. Unfortunately, the Federal Trade Commission, which is tasked with preventing consumer data abuses, has not been given the resources to keep pace with this tech based economy.

Professor Vladeck, we will hear from you, but I think you—have in your opening remarks that basically now the FTC's docket is dominated by these technology issues. The truth is that our economy has changed significantly, and the Federal Trade Commission has neither the adequate resources nor the technological expertise at the FTC to adequately protect consumers from harm.

While the Commission is responsible for keeping up with the latest technology companies in the world, according to today's testimony, "it has fewer than 10 employees on staff with the right technology expertise." The FTC simply does not have the tools to fend off privacy attacks, data breaches, Internet scams, ransomware, digital abuses that threaten consumers and our economy. It is not to say the FTC hasn't done some good work. But when we look at the volume of what we are facing, it is clear you are under—they are underresourced.

Even where the FTC has taken enforcement actions against companies, the companies continue to violate those FTC orders, which is beyond frustrating. Even though the FTC has been able to use their current authority of unfair and deceptive practices, companies like Facebook or others may gladly pay a \$5 billion fine when actually they can still make over \$70 billion a year from some of these same practices. So, compliance. We need compliance. Compliance with existing laws or compliance with new rulemaking or compliance with a new privacy law will be insufficient if the FTC is not well resourced, technology sophisticated, and the policeman on the beat of the information age.

The U.S. Department of Commerce estimated that the digital economy accounted for 9.6 percent of GDP in 2019, and it grows annually at a rate of 5.2 percent. This means we are just going to continue to be ever dependent on this economy. I am not even going to spend time talking about at length the great effect of State actors attacking our systems. The fact that we are—consumers are less vulnerable to these events. But the economy of today is that—the digital economy generates \$2 trillion annually. So it will con-

tinue to be a target. As the economy grows, the volume of data collected about Americans and the amount of data that will be stored is staggering.

Last Congress, I introduced the Consumer Online Privacy Act alongside my colleague Schatz, and Klobuchar, Markey, that would have established a new privacy bureau at the FTC to serve as a consumer privacy watchdog. And I am pleased that the Budget Reconciliation Act that we are now considering in both the House and the Senate has a call for action here by giving \$1 billion to the FTC to establish this bureau over 10 years, to hire the technologists, the data scientists, needed to keep pace with these digital threats. I know my Republican colleagues in the SAFE DATA Act also called for a similar amount of money to be spent by the FTC for privacy and data security.

And as such, companies like Microsoft and others have called for greater investments. Today's witnesses, I know, will also underscore this need. Two of our witnesses, Professor David Vladeck and Ms. Maureen Ohlhausen have served in senior positions at the FTC and have been on the front lines of enforcement actions against companies that misused or neglected their security of personal data. We value their insights and how harm at the FTC—how harm can be done, and that tools and resources are needed at the FTC to hold companies accountable.

Mr. Vladeck, in your written testimony, you said the Bureau of—New Privacy Investment Bureau could be a real game changer. Mr. Soltani, who is going to be joining us virtually, was one of the first technology experts hired by the FTC, and I know he's been sounding the alarm for years about the need to get the right resources, more technologists so the FTC can deliver more, so I look forward to asking him questions about that.

And Mr. Reed, I was pleased to read your testimony, that you have a strong statement in support of first time civil penalty enforcements for the FTC in cases of privacy violations. So thank you all for being here. Thank you for all the work all of you have done on this important issue. And now I will turn it over to my friend and colleague, Senator Wicker, the Ranking Member, for his opening statement.

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

Senator WICKER. Thank you, Senator Cantwell, for convening this hearing. And we do have a distinguished panel and I look forward to their testimonies. Last Congress, this committee heard from multiple stakeholders representing diverse views on how best to protect consumers' data privacy and security in the United States.

We received testimony from current and former officials from the FTC, representatives from the business community, and academia, and privacy advocates who all testified about the vast economic and social benefits of data. They also spoke about the need for strong, clear, and consistent data protection rules for the Nation's job creators and about shortcomings in our existing data privacy and security laws. Since the full committee last convened on this

topic over a year ago, the need for strong data privacy rules has become more urgent.

In response to the COVID-19 pandemic, millions of Americans have shifted their normal activities to online. This has resulted in more consumer data and personal information flowing throughout the economy than ever before. Without a national data privacy law in place, Americans will continue to face a growing risk of having their personal data exposed and potentially exploited. We are already seeing this happen. As the Chair has mentioned, earlier this year, the FTC reported that identity theft increased by almost 3,000 percent in 2020. Cyber-attacks and data breaches are also on the rise. Recent news reports show an uptick in exploitive data practices by social media targeting children and teens.

And there are near daily accounts of entities misusing consumers' personal data or attempting to process their data in discriminatory ways. These developments are deeply troubling and further highlight the need for strong data protection rules. Without these safeguards, we risk losing consumers' trust in the Internet marketplace and undermining our national security and technological leadership abroad.

Fortunately, Congress still has an opportunity to act to develop bipartisan national privacy legislation. In doing so, the United States would join more than 100 countries who already have a baseline privacy law, including China. In July, Senator Blackburn joined me in introducing a data privacy bill, the SAFE DATA Act, as a starting point to resume negotiations. And I am encouraged that this morning the Chair of this committee spoke favorably about a provision in that Act. Once again, I invite the Administration to work with Senator Cantwell and me to make a comprehensive data privacy law a reality.

I call on the President to appoint someone, a specific person among his senior staff to be a liaison to Congress on this issue and to prioritize the enactment of a data privacy law this year. This is not only essential to a thriving digital economy, but it would also demonstrate to our allies around the world a serious and sincere commitment to the value of data protection as we seek to replace the EU, U.S. Privacy Shield, preserve transatlantic data flows, and enter into the new bilateral partnership on trade and technology.

Today's hearing is an opportunity to discuss how to address certain issues in privacy legislation such as data security and enforcement. I hope our witnesses will speak to ways in which Congress can materially improve data security without imposing costly one size fits all mandates that would ignore an entity's unique data collection practices. I also hope witnesses will speak to what enforcement mechanisms offer the best way to ensure that requirements in privacy law are met and data protections are enforced. Last Congress, I proposed incorporating a narrow private right of action into a bipartisan privacy legislation, and I remain open to that idea.

I welcome feedback from witnesses on how a narrow private right of action could be constructed without stifling innovation and marketplace competition or leading to unjustified financial windfalls for plaintiffs' attorneys. Today's hearing is also an opportunity to discuss how to ensure the FTC is properly resourced to enforce a data privacy law. I am sure witnesses will want to discuss what

additional funding staff and technology expertise the Commission were required to enforce the law effectively.

Finally, it is worth emphasizing that Congress, not the FTC, is responsible for developing a comprehensive national data privacy law. Only Congress can develop long-standing data protections for consumers that meaningfully safeguard their personal information. Anything short of Congressional action would create significant regulatory uncertainty for businesses and confuse consumers about the scope and durability of their privacy rights. Americans deserve to have their data protected. The time for Congress to act to pass Federal data privacy legislation is now. And I am—I can say that the Chair and I are united in that belief. I would like to take a moment to ask unanimous consent.

I have here, Madam Chair, a letter signed by over 20 associations representing hundreds of companies and organizations requesting that Congress pass a bipartisan national privacy law. I ask unanimous consent that they be entered into the record at this point.

The CHAIRWOMAN. Without objection.
[The information referred to follows:]



September 27, 2021

The Honorable Maria Cantwell, Chair
 The Honorable Roger Wicker, Ranking Member
 U.S. Senate Committee on Commerce, Science, and Transportation
 Washington, D.C. 20510

Dear Chair Cantwell and Ranking Member Wicker,

The undersigned civil rights, civil liberties, and consumer protection organizations sincerely thank you for your work to ensure better protections for consumer data privacy and security. To that end, we urge you to, as proposed by the House Committee on Energy and Commerce, allocate at least \$1 billion in the Build Back Better Act to create a new division in the Federal Trade Commission (FTC) to protect data privacy and prevent security abuses.¹ For far too long, Congress has failed to sufficiently fund the FTC to do the massive job with which it is tasked. The agency is overdue for an influx of resources to help it play catch-up to the modern economy.

The FTC is vastly underfunded and understaffed, particularly in comparison to the large, well-funded entities that it is tasked with regulating. Currently, the FTC only has 1,100 full-time employees (FTEs) to pursue both its competition and consumer protection missions.² This number has been roughly flat over the past twelve years, and represents a substantial decrease from 1,746 FTEs in 1979. Put another way, since that time, the economy has grown nearly three times while the FTC's capacity has decreased 37 percent. In contrast, in 2020, Facebook alone had total revenues of nearly \$86 billion and nearly 60,000 employees.³

This increased funding for the FTC is especially important because it will enable the Commission to protect people of color and low-income communities from identity theft, fraud, scams, and exploitation. Privacy rights help prevent people from being treated unfairly based on who they are—privacy rights are civil rights.⁴ Unfair and deceptive data practices disproportionately harm people of color and low income communities. In an Internet-driven economy, equal opportunity depends on fair data practices. As the FTC recently wrote,

¹ Committee on Energy and Commerce, Budget Reconciliation Legislative Recommendations Relating to FTC Privacy Enforcement, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Subtitle%20O_FTC%20Privacy%20Enforcement.pdf.

² *FTC Appropriation and Full-Time Equivalent (FTC) History*, FED. TRADE COMM'N (last visited Apr. 16, 2021), <https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation>.

³ *Facebook Reports Fourth Quarter and Full Year 2020 Results*, FACEBOOK (Jan. 27, 2021), <https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx>.

⁴ See *Am. for Prosperity Found. v. Bonta*, 141 S.Ct. 2373, 2382 (2021) (discussing *NAACP v. Alabama*, 357 U.S. 449 (1958)).

“apparently ‘neutral’ technology can produce troubling outcomes—including discrimination by race and other legally protected classes.”⁵

For years, advocates have called on legislators to adopt a federal privacy law, but there is still no comprehensive federal law that governs the collection, use, and sharing of consumer data, even as industry’s data collection and monetization practices have become ever more invasive. Nor is there a federal law that specifically requires businesses to keep that data secure from hackers, despite myriad breaches, including a recent breach at T-Mobile involving the Social Security numbers of millions of consumers.⁶ These breaches can lead to identity fraud, which cost consumers an estimated \$13 billion in 2020 alone.⁷ This lack of a federal privacy law has become particularly glaring as the European Union has established its own comprehensive data protection framework, the GDPR, and states such as California and Colorado have adopted baseline privacy protections for their residents.

While the FTC can take action against privacy and security violations under its authority to address unfair and deceptive acts and practices, it lacks the authority to issue civil penalties for first-time violations, and the courts have knocked down its ability to prevent wrongdoers from profiting from their fraudulent acts and to repay the victims under its 13(b) authority.⁹ Advocates have previously urged you to strengthen the FTC’s authority in these areas, making clear that these restrictions clearly hamper the FTC’s enforcement.¹⁰

This funding will be crucial in enabling the FTC to meet its responsibilities to protect consumer privacy. Recognizing the need for federal guidelines to rein in data collection, use, and sharing—and the need to give the FTC the authority to issue civil penalties for first-time violations—a recent executive order encouraged the FTC to pursue a rulemaking to address “unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy.”¹¹ However, given the FTC’s current limited funding, the agency will be curtailed in its ability to engage in that rulemaking while also engaging in enforcement actions against companies that violate people’s privacy.

⁵ Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company’s Use of AI*, FED. TRADE COMM’N (April 19, 2021), <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.

⁶ *T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack*, T-MOBILE (Aug. 17, 2021), <https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation>.

⁷ *Total Identity Fraud Losses Soar to \$56 Billion in 2020*, Javelin (Mar. 23, 2021), <https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-Losses-Soar-to-56-Billion-in-2020>.

⁹ *AMG Capital Management, LLC et al. v. Fed. Trade Comm’n* (Apr. 22, 2021), https://www.supremecourt.gov/opinions/20pdf/19-508_16gn.pdf.

¹⁰ Testimony of Anna Laitin, Consumer Reports, Before the United States House of Representatives Committee on Energy & Commerce, Subcommittee on Consumer Protection and Commerce, Hearing on “The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers” (April 27, 2021), <https://docs.house.gov/meetings/IF/IF17/20210427/112501/HHRG-117-IF17-Wstate-LaitinA-20210427.pdf>.

¹¹ The White House, Executive Order on Promoting Competition in the American Economy (July 9, 2021), <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/>.

The FTC also needs funds to hire more technologists to fulfill its critical mission, as the FTC is expected to have the technical expertise and sophistication to meaningfully check the big tech companies that dominate the tech sector. In 2015, the Commission created the Office of Technology Research and Investigation as a way of levelling the playing field and empowering the FTC to better tackle abuses from technology companies.¹² Despite its wide-ranging mission, the FTC did not hire any new FTEs, so it was largely staffed by shifting personnel from other parts of the office. Even today, OTECH only has a handful of employees to support all five departments in the Bureau of Consumer Protection.

The federal government has stalled in reining in giant technology companies, even as these businesses have grown bigger and more powerful. Now, legislators have a prime opportunity to help empower the FTC to go after companies that freely collect and monetize consumer data without their knowledge or consent. We urge you to advance the \$1 billion proposal to protect data privacy and prevent security abuses.

Respectfully Submitted,

Access Now
 American Civil Liberties Union
 Asian Americans Advancing Justice – AAJC
 Center for American Progress
 Center for Democracy & Technology
 Center for Digital Democracy
 Center on Privacy & Technology at Georgetown Law
 Common Cause
 Common Sense
 Consumer Action
 Consumer Federation of America
 Consumer Reports
 Cyber Collective
 Electronic Privacy Information Center (EPIC)
 Fairplay
 Free Press Action
 Greenlining
 Hispanic Technology & Telecommunications Partnership
 Lawyers' Committee for Civil Rights Under Law
 Media Alliance
 National Hispanic Media Coalition
 New America's Open Technology Institute
 Privacy Rights Clearinghouse

¹² *FTC Seeks Technologists for New Research, Investigations Office*, FED. TRADE COMM'N (Mar. 23, 2015), <https://www.ftc.gov/news-events/press-releases/2015/03/ftc-seeks-technologists-new-research-investigations-office>.

Public Knowledge
Public Citizen
Ranking Digital Rights
Revolving Door Project
Stop Online Violence Against Women

cc: Members, U.S. Senate Committee on Commerce, Science, and Transportation



September 28, 2021

The Honorable Maria Cantwell
Chair
Committee on Commerce, Science, and
Transportation
United States Senate
Washington DC, 20515

The Honorable Roger Wicker
Ranking Member
Committee on Commerce, Science, and
Transportation
United States Senate
Washington DC, 20515

RE: Senate Commerce Committee Hearing on "Protecting Consumer Privacy"

Dear Chair Cantwell, Ranking Member Wicker, and Members of the Committee:

On behalf of the Computer & Communications Industry Association (CCIA)¹, I write regarding the Committee's upcoming hearing on "Protecting Consumer Privacy." CCIA welcomes the Committee's focus on the important issue of consumer privacy and the vital need to enact comprehensive federal privacy legislation. In recent years, increasing public attention to the treatment of consumers' personal data, the adoption of inconsistent state-level privacy laws, and pressures to American digital trade and economic competitiveness produced by foreign data governance regimes have all underscored the necessity for the US to adopt a strong and consistent framework for the responsible treatment of consumer information throughout the economy.

While the upcoming hearing is a positive development and valuable opportunity to hear from expert witnesses on consumer privacy interests, many stakeholders are hopeful for announcements on progress towards the adoption of comprehensive privacy legislation. Members of the Senate Commerce Committee have introduced several well-considered consumer privacy bills including the *Consumer Online Privacy Rights Act*, the *Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act*, and the *Consumer Data Privacy and Security Act*.² These bills share many common attributes for establishing consumer data privacy rights, organizational accountability mechanisms, and robust enforcement processes. We urge the Committee to move forward in a bipartisan manner on these shared principles to swiftly advance a comprehensive consumer privacy framework this Congress.

¹ CCIA is an international nonprofit membership organization representing companies in the computer, Internet, information technology, and telecommunications industries. Together, CCIA's members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue. CCIA promotes open markets, open systems, open networks, and full, fair, and open competition in the computer, telecommunications, and Internet industries. A complete list of CCIA members is available at <http://www.cciainet.org/members>.

² S.2968 (116th Congress); S.2499 (117th Congress); S.1494 (117th Congress).

CCIA appreciates the Committee's recognition of the central role that the Federal Trade Commission ("FTC" or "The Commission") does and should continue to play in the protection of consumer privacy and offers the following comments for consideration as the Committee moves forward on this important subject.

The Federal Trade Commission and Protecting Consumer Privacy

The Commission has a proven track record of independence and bipartisan collaboration in protecting Americans' privacy and has taken hundreds of enforcement actions on privacy and security by virtue of both its authority to police "unfair and deceptive acts and practices" and pursuant to sector-specific privacy laws such as the Children's Online Privacy Protection Act and Fair Credit Reporting Act. These actions have included approaches such as requiring the implementation of comprehensive privacy and security programs, regular assessments by independent experts, monetary redress to consumers, and the deletion of illegally obtained data.³ An enduring strength of the Commission is its ability to leverage a varied toolkit to take flexible, appropriate action in the context of an alleged privacy or security violation.

In considering avenues for equipping the Commission with additional resources and enforcement authority, consumer privacy interests will be best served if advanced as part of the enactment of comprehensive federal privacy legislation. Establishing clear and consistent baseline rules for the fair and transparent use of personal information will protect individuals, give organizations predictability in meeting their compliance obligations, and enable the Commission to most effectively deter and enforce violations of consumer privacy rights. CCIA recommends that the Committee consider the following approaches to augmenting the Commission's enforcement capacity as part of the adoption of a national privacy framework.⁴

Commission Resources:

A recent report revealed that the Federal Trade Commission employs approximately 40 Full-Time Equivalents (FTEs) focused on privacy and security issues, lagging far behind many foreign privacy regulatory agencies.⁵ CCIA supports the allocation of additional resources to expand the Commission's existing privacy work, not limited to conducting investigations and undertaking enforcement actions, but also to carry out its important roles in hosting educational workshops,

³ See Federal Trade Commission, "Privacy & Data Security Update: 2020" (May, 2021), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

⁴ For additional consideration on the substance of a modern consumer privacy framework, see CCIA's letter to the Committee dated September 23, 2020 available at <https://www.cciainet.org/wp-content/uploads/2020/09/CCIA-Statement-for-the-Record-on-Senate-Commerce-Privacy-Hearing-9.23.pdf>.

⁵ Federal Trade Commission, "FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security" (2020), www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf.

issuing public reports, and completing the necessary studies to quantitatively evaluate the benefits and harms of particular data practices to ensure an empirically grounded regulatory approach.

While additional funding for the Commission is advisable, we encourage Congress to ensure that any allocation of new resources will fulfill identified needs. Privacy enforcement has been effectively carried out through the Bureau of Consumer Protection, and lawmakers should carefully consider whether organizational readjustments will help the Commission fulfill its privacy role. Recent proposals including the creation of a new privacy bureau within the Commission or the creation of three new privacy focused units are worth exploring in greater detail.⁶

Commission Enforcement Authority:

In addition to ensuring that the Commission has adequate resources to protect consumer privacy, Congress should consider augmenting the Commission's regulatory authority to enforce comprehensive privacy legislation in the following ways.

First, as part of enacting comprehensive privacy legislation, Congress should consider granting targeted APA rulemaking authority to the Commission to provide greater clarity and ensure the statutorily mandated federal privacy framework remains fit for purpose in light of changes in technology and business practices. For any grant of rulemaking it will be important to delineate specific definitions and issues for which the promulgation of federal rules will promote understanding and compliance and protect consumers. A protracted, expansive rulemaking process lacking statutory guardrails and grounding could have the impact of turning compliance into a moving target, creating confusion for both businesses and consumers, and risk needlessly politicizing the rulemaking process. Elected members of Congress are best positioned to negotiate the critical substantive policy determinations that will animate a durable and comprehensive privacy framework and deliver a win for American consumers and American innovation and economic competitiveness.

Second, a privacy framework should ensure that consumers can feel confident that their personal data is protected, no matter who is using it or for what purposes. Therefore, in establishing comprehensive, tech-neutral rules, Congress should also grant the FTC jurisdiction over common carriers and non-profit organizations and eschew sector-specific carveouts. Organizations currently excluded from FTC enforcement nevertheless can process data in ways that raise significant privacy and security concerns.

⁶ See Committee on Energy and Commerce, "Budget Reconciliation Legislative Recommendations Relating to FTC Privacy Enforcement" (September, 2021), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Subtitle%20O_FTC%20Privacy%20Enforcement.pdf; Chairman Simons, Letter to the Subcommittee on Consumer Protection and Commerce (Apr. 1, 2019), <https://congress.gov/116/meeting/house/109415/documents/HHRG-116-IF17-20190508-SD010.pdf>.

Finally, the FTC's enforcement capacity should be expanded by granting first-time fining authority that the Commission may pursue, where appropriate, for violations of the federal law and implementing rules. The Commission already exercises such authority effectively and responsibly in carrying out enforcement of the Children's Online Privacy Protection Rule and the Fair Credit Reporting Act.

Conclusion

We look forward to working with you and other stakeholders on a strong and flexible privacy framework for the digital economy. Should you have additional questions, please feel free to reach out to Arthur Sidney, Vice President of Public Policy (asidney@ccianet.org) and Keir Lamont, Policy Counsel (klamont@ccianet.org). Thank you again for holding this important hearing.

Sincerely,

Arthur Sidney
Vice President of Public Policy
Computer & Communications Industry Association



September 28, 2021

The Honorable Maria Cantwell
Chair
U.S. Senate Committee on Commerce,
Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Roger Wicker
Ranking Member
U.S. Senate Committee on Commerce,
Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

RE: Hearing on “Protecting Consumer Privacy” (September 29, 2021)

Dear Chair Cantwell and Ranking Member Wicker:

The Main Street Privacy Coalition (MSPC), a coalition of 19 national trade associations representing more than a million American businesses,¹ appreciates your focus on the need for federal data privacy protections and offers this statement for the hearing record. MSPC is comprised of a broad array of national trade associations representing businesses that line America’s Main Streets. From retailers to REALTORSTM, hotels to home builders, grocery stores to restaurants, gas stations to travel plazas, and self-storage to convenience stores, MSPC member companies interact with consumers day in and day out. Our members’ businesses can be found in every town, city and state in our nation, providing jobs, supporting our economy and serving Americans as a vital part of their communities.

Collectively, the industries that MSPC member associations represent directly employ nearly 34 million Americans and constitute over one-fifth of the U.S. economy by contributing \$4.5 trillion (or 21.8%) to the U.S. gross domestic product (GDP). Our success depends on maintaining trusted relationships with our customers and clients: trust that the goods and services we provide are high quality and offered at competitive prices; and trust that the information customers provide to us is kept secure and used responsibly. For these reasons, our associations are actively engaged in the discussions surrounding data privacy and continue to work together to support Congress’s enactment of a comprehensive and uniform federal data privacy law.

MSPC is dedicated to the enactment of a federal data privacy law that creates privacy obligations for all businesses handling consumers’ personal information, and we support the Committee’s efforts to bring greater attention to the need for a such a law. We strongly believe that the views of Main Street businesses should be considered on this issue given that Main Street represents the backbone of the United States economy. Main Street businesses, many of whom have remained open to continue to serve consumers during the COVID-19 pandemic, will bear the full burden of regulatory obligations under proposed privacy bills the committee may consider this Congress. In the past, bills considered in Congress largely exempted telecommunications companies and big tech service providers from similar obligations to protect consumer privacy. Further, despite the bipartisan desire to enact federal data privacy legislation to protect consumers comprehensively, much of the proposed legislation to date has focused on

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

Main Street Privacy Coalition
 September 28, 2021
 Page 2

requiring Main Street businesses to protect consumers' data but not financial institutions, data brokers and social media companies that routinely process more sensitive consumer information. MSPC therefore urges the Committee to hear from and work with all stakeholders to advance a federal data privacy bill that applies equivalent provisions to all businesses handling consumers' personal information.

Virtually every industry sector – whether consumer-facing or business-to-business – handles significant volumes of consumer information. To protect Americans comprehensively, federal data privacy legislation should ensure that all industry sectors are covered and that there are no privacy loopholes that leave consumers unprotected when their personal data is handled by any business. All of the companies involved in handling the chain of personal data should have legal obligations to protect it under a federal privacy law and honor consumers' privacy requests. We should not rely on private contracts to create those legal obligations between parties, particularly between businesses that vary greatly in size and bargaining power (i.e., Main Street businesses versus global service providers).

MSPC has been concerned with provisions in the privacy legislation the Committee has considered in the past that would exempt service providers and third parties from statutory obligations to honor consumer rights exercised to protect their privacy. These exemptions for service providers would be extended to businesses in the telecommunications industry and technology companies. There are more effective ways to protect Americans' privacy. For example, privacy bills could be drafted with the premise that each business handling consumers' personal data should have statutory requirements to do what it is able to do to protect the consumer privacy established in the legislation without making consumer-facing businesses responsible for privacy violations by businesses that serve them and that they cannot control, such as much larger service providers. Legislation that takes this approach would more effectively secure the consumer rights it establishes and treat industry sectors fairly by making them responsible for their own conduct.

Privacy responsibilities should not simply be shifted from one industry sector onto another – not only because that is an ineffective way to protect consumer information but also because it is manifestly unfair to businesses that bear the brunt of those burdens for what should be the other businesses' own obligations to the consumer. Because our members include small businesses, they know that all too often powerful businesses within the telecom and tech industry sectors may use their superior market position to shift what should be their responsibilities onto their clients, typically leaving Main Street businesses with outsized compliance burdens and costs. If this approach is taken by Congress, it will leave holes in consumer privacy rights because federal enforcement agencies will have no effective way to compel service providers or third parties to comply with the law. Moreover, Main Street businesses will lack the financial and legal resources to hold them accountable for privacy practices that harm their customers.

MSPC has additionally been concerned with the exemption for financial institutions and other entities subject to the Gramm Leach Bliley Act (GLBA) from the consumer privacy protections in federal legislation. GLBA, a law enacted in 1999 that is significantly outdated in its extremely narrow privacy protections, which do not provide anything close to the privacy protections that the Committee's previously considered legislation extends to consumers. For instance, GLBA requires that an entity sharing consumer financial data with unaffiliated third parties for marketing purposes provide an annual opt-out notice in writing, which most

Main Street Privacy Coalition
 September 28, 2021
 Page 3

consumers likely never read. GLBA does not, however, require any access, correction or deletion of consumers' financial data upon request, as past privacy bills in this Committee would require of every other consumer-facing business on Main Street that is not a bank or credit union. Exemptions for financial institutions and other entities subject to GLBA permit these select consumer-facing businesses to avoid proposed federal privacy bills' requirements and leave consumers unprotected while feeling a false sense of security they are fully covered.

Despite these concerns with past bills, we support and appreciate several Committee members' recent calls for Congress to enact a uniform, preemptive federal privacy bill that sets a national standard for consumer privacy protections. Such a privacy law would aid consumers and businesses alike by ensuring consumer privacy protections are the same regardless of the state in which a consumer resides or a business is located. The increasing patchwork of newly enacted state privacy laws is one of the key reasons a uniform federal privacy law is needed today.

With that in mind, we believe federal privacy legislation should establish a uniform, nationwide and consumer-centric federal data privacy law that embodies these principles:

1. Industry Neutrality and Equal Protection for Consumers Across Business Sectors – Federal data privacy frameworks and legislation should apply requirements to all industries that handle personal data and not place a disproportionate burden on certain sectors of the economy while simultaneously alleviating other sectors from providing equal protection of consumer data. An equivalent data privacy standard should apply, regardless of whether a business directly collected data from a consumer or obtained it in a business-to-business transaction.
2. Direct Statutory Obligations (Rather than Contractual Requirements Alone) for All Entities that Contact Consumer Data – Effective consumer protection regulations cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. Data service providers and other third parties need direct statutory obligations to ensure they comply with relevant privacy laws, particularly those offering transmission, storage, analytical processing or other consumer data services for thousands of small businesses.
3. Preservation of Customer Rewards and Benefits – Any federal data privacy framework should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships and set the terms of those relationships. Federal law should include safe harbors to ensure that consumers can purchase, or otherwise obtain, the goods and services they want by taking advantage of benefits, incentives or enhanced services they earn from being loyal customers, even if other customers choose not to engage in such programs.
4. Transparency and Customer Choice – Consumers deserve to know what categories of personal data businesses collect and how that data is generally used. These policies should be clearly disclosed in company privacy policies readily accessible to consumers. These obligations should apply to all businesses handling consumers' personal data, including service providers and third parties.

Main Street Privacy Coalition
September 28, 2021
Page 4

5. Accountability for Business's Own Actions - Privacy law should not include terms that could potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of a business partner. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability if other types of businesses do not fulfill their own obligations under the law.
6. Data Security & Breach Notification – A federal data privacy law should include a reasonable data security standard for all businesses handling consumer data, as well as a uniform process for businesses suffering a data security breach to notify affected individuals. Currently, consumer-facing industry sectors are required to comply with 54 state and U.S. territorial laws on data breach notification requirements, and nearly half of the states have enacted data security laws. However, financial institutions and service providers are often exempt from these state breach notice requirements. All businesses handling consumers' data should be required to protect personal data and provide notice of their own security breaches when they occur.
7. Establishing Uniform Nationwide Rules and Enforcement for Data Privacy – Congress should create a sensible, uniform federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws by enacting a set of nationwide rules for all businesses handling consumers' personal data is necessary to achieve the important, national public policy goal of uniform consumer privacy protections.

As you consider ways to advance federal data privacy legislation, the members of the MSPC urge you to include these key principles in your bills and continue to solicit input from all affected industries and from businesses of all sizes during the legislative process. We look forward to a constructive dialogue with you on these matters as you craft federal data privacy legislation in the remainder of this session and in the next Congress.

Sincerely,
The Main Street Privacy Coalition

cc: The Honorable Charles E. Schumer
The Honorable Mitch McConnell
Members of the Committee on Commerce, Science, and Transportation



September 28, 2021

The Honorable Maria Cantwell
U.S. Senate Committee on Commerce,
Science, and Transportation
Washington, DC 20510

The Honorable Roger Wicker
U.S. Senate Committee on Commerce,
Science, and Transportation
Washington, DC 20510

Dear Chair Cantwell and Ranking Member Wicker:

The National Retail Federation applauds the Senate Commerce Committee's holding of a hearing entitled "Protecting Consumer Privacy" on September 29, 2021. To protect American consumers and their information comprehensively, we urge the Committee to move forward with privacy legislation and not leave this important work to the Federal Trade Commission alone without a clear statutory framework adopted by Congress.

NRF, the world's largest retail trade association, passionately advocates for the people, brands, policies and ideas that help retail thrive. From its headquarters in Washington, D.C., NRF empowers the industry that powers the economy. Retail is the nation's largest private-sector employer, contributing \$3.9 trillion to annual GDP and supporting one in four U.S. jobs — 52 million working Americans. For over a century, NRF has been a voice for every retailer and every retail job, educating, inspiring and communicating the powerful impact retail has on local communities and global economies.

Federal privacy legislation is necessary to establish uniform, national standards that protect all Americans' personal information wherever it is collected and used, regardless of the state where a consumer resides or a business is located. Further, federal legislation should protect consumers by applying equivalent data privacy requirements to *all* businesses handling their personal data, consistent with consumers' expectations, and thereby avoid the pitfalls of privacy bills that exempt service providers, third parties and financial institutions from meeting the same standards that apply to Main Street businesses that are serving consumers. Such exemptions would create loopholes that leave Americans unprotected while providing them a false sense of security that all businesses are federally required to protect their data privacy to the same extent. Finally, it is critically important for American commerce that Congress act to establish a clear framework that embodies the Main Street [privacy principles](#) we strongly support.

We look forward to working with you on bipartisan data privacy legislation.

Sincerely,

David French
Senior Vice President
Government Relations

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com



September 29, 2021

The Honorable Maria Cantwell
Chair
U.S. Senate Committee on Commerce, Science & Transportation
420-A Hart Senate Office Building
Washington, DC 20510

The Honorable Roger Wicker
Ranking Member
U.S. Senate Committee on Commerce, Science & Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

RE: Hearing on Protecting Consumer Privacy

Dear Chair Cantwell and Ranking Member Wicker:

Today's hearing focuses on a critical issue: how to protect consumer privacy. Consumers today share their personal information with countless businesses in the course of using everyday products and services, both online and offline. Consumers deserve to know their personal information is being used responsibly.

A strong, comprehensive federal privacy law is the best way to ensure consumers have important rights over their personal data and to limit how businesses can collect, use, and share that information. We commend the Senate Commerce Committee for your bipartisan leadership on consumer privacy legislation, and we urge you to continue the important work to enact a strong and comprehensive federal consumer privacy law.

BSA | The Software Alliance is the leading advocate for the global software industry.¹ Our members are enterprise software companies that create the business-to-business technology products and services that power the digital transformation of companies in other industry sectors, including through cloud storage services, customer relationship management software, human resource management programs, identity management services, and remote collaboration software.

Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations. BSA companies are not built on business models that monetize users' data; our members license software

¹ BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zendesk, and Zoom.

Page 2

and sell services, as partners to businesses of all sizes across every industry in the economy.

I. The Need For A Strong, Comprehensive Federal Consumer Privacy Law

BSA supports enactment of a strong, comprehensive federal privacy law that provides confidence to consumers that their data will be used responsibly – and ensures that companies that violate their obligations are subject to strong enforcement. We believe federal privacy legislation should achieve three goals: (1) establish consumers' rights in their personal data, including the right to access, correct, and delete that data; (2) impose strong obligations on companies to safeguard consumers' data and prevent misuse; and (3) provide strong, consistent enforcement.²

In each of these areas, a federal privacy law can – and should – build on the protections and obligations that states have advanced and enacted. State privacy laws share many core policies, including:

- *Consumer Rights.* State consumer privacy laws include important consumer rights, including access, correction, and deletion, which should also be included in any federal privacy law.
- *Obligations on businesses.* State consumer privacy laws also place meaningful limits on how businesses can collect, use, and share consumers' personal information. A federal law should build on those obligations, to ensure that companies are required to use consumers' personal data in ways they expect. For example, although consent obligations are an important aspect of any privacy law, we believe a federal privacy law should avoid relying on consent alone, and instead combine other guardrails such as data minimization, purpose specification, and data security obligations, to further safeguard consumers' personal data.
- *Enforcement.* State consumer privacy laws also recognize the need for strong regulatory enforcement. We believe that a federal privacy law should not be enforced by a single regulator, but by federal and state agencies working together. In addition to the FTC, state attorneys general should be empowered to enforce a federal privacy law, which will complement their longstanding privacy enforcement efforts at the state level.

We also appreciate the Committee's leadership in developing comprehensive federal privacy legislation, including the Consumer Online Privacy Rights Act ("COPRA") and the Setting an American Framework to Ensure Data Access, Transparency, and Accountability ("SAFE DATA") Act.

Earlier this year, BSA joined with the National Consumers League, Common Sense Media, and the 21st Century Privacy Coalition to support federal legislative efforts to enact a strong new data privacy law. We believe there is significant common ground on protecting consumer privacy and we remain committed to collaborating with leaders in Congress to create clear, comprehensive federal privacy protections.

² See Testimony of Victoria Espinel, President and CEO of BSA | The Software Alliance, before the Senate Committee on Commerce, Science and Transportation, at Hearing on Policy Principles for a Federal Data Privacy Framework in the United States, February 27, 2019, *available at* <https://www.commerce.senate.gov/services/files/1DEC081B-5947-4FEB-B3E1-E9DF65866321>.

Page 3

II. The Role of the Federal Trade Commission

We also welcome the Committee's focus on ensuring the Federal Trade Commission has the resources it needs to safeguard consumers' privacy.

BSA supports the Federal Trade Commission's strong role in protecting consumer privacy. The FTC has demonstrated that it is highly capable of overseeing and enforcing existing consumer privacy protections, as is evident from the more than 150 privacy and data security enforcement actions the agency has brought under Section 5 of the FTC Act.³ The FTC has also developed a deep understanding of the complexities of the digital economy and has generally observed the principle of bringing cases that remedy and deter harmful conduct, rather than punishing technical lapses. Given its strong record, the FTC should maintain its leadership role as the primary federal enforcer of consumer privacy protections and it should have the tools and resources necessary to carry out its mission effectively.

Effective enforcement is critical to ensuring that organizations meet their commitments and legal obligations and to deterring potential violations. BSA supports giving the FTC new authorities to enforce a comprehensive privacy law, including targeted rule-making authority, the ability to fine first-time violators, and additional funding and staff, which we recognize are key aspects of several of consumer privacy bills put forward by members of this Committee. Ultimately, we believe the FTC needs more than resources to effectively address consumer privacy – it also needs a strong, comprehensive national consumer privacy law to enforce.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the Committee on these important issues.

Sincerely,



Aaron Cooper
Vice President, Global Policy
BSA | The Software Alliance

³ See FTC, Privacy and Data Security Update 2020, at 2-3, available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-updater2010524_privacy_and_data_security_annual_update.pdf

KIRSTEN GILLIBRAND
NEW YORK
SENATOR
RUSSELL SENATE OFFICE BUILDING
SUITE 478
WASHINGTON, DC 20510-3205
202-224-4451

United States Senate
WASHINGTON, DC 20510-3205

COMMITTEES:
ARMED SERVICES
ENVIRONMENTAL AND PUBLIC WORKS
AGRICULTURE
SPECIAL COMMITTEE ON AGING

September 29th, 2021

Dear Chair Cantwell, Ranking Member Wicker, and Members of the Senate Committee on Commerce, Science, and Transportation,

Thank you for holding this important hearing, "*Protecting Consumer Privacy*," which will further elevate this important topic in Congress and help us craft sustainable legislative solutions. It is high time that the United States implement comprehensive policies aimed at protecting our right to privacy. I commend the leadership of the House Committee on Energy and Commerce and the Senate Committee on Commerce, Science, and Transportation as they usher a proposal through Congress to award up to \$1 billion for the Federal Trade Commission (FTC) to establish a bureau dedicated to improving data security and privacy. This new bureau would be a critical first step towards the robust federal privacy enforcement regime that Americans need in the digital age. Even with this funding, there is still more that needs to be done to ensure Americans' privacy is protected and that the United States remains one of the most competitive technology sectors in the world.

Unrestricted data collection can directly impact the opportunities for an individual to secure employment, insurance, credit and housing, among others. The United States is one of the few democracies in the world, and the only member of the Organization for Economic Co-operation and Development, without a federal data protection agency. As data and technology continue to challenge existing paradigms of society and democracy, the U.S. needs a federal agency focused on safeguarding the personal data and civil liberties of Americans. This is why it is imperative we create an independent, consumer watchdog agency to give Americans control over their data, a Data Protection Agency. As Congress and its committees continue to consider policies regarding data privacy and technology, I urge passage of *S. 2134 - the Data Protection Act* and the legislation's establishment of an independent agency dedicated to protecting Americans against individual and collective privacy harms.

The *Data Protection Act*, which I introduced alongside Senator Brown, Chair of the Senate Committee On Banking, Housing, and Urban Affairs, and have championed with Representatives Anna Eshoo (CA-18), member of the House Energy and Commerce Committee, and Zoe Lofgren (CA-19), member of the House Judiciary Committee, aims to create an agency with the specific mission of protecting our right to privacy. The bill outlines the scope and purpose of the proposed Data Protection Agency, as well as an administrative structure and important definitions regarding privacy harm and data aggregators.

Considerations for Proposed FTC Bureau of Privacy and Data Security

If the \$1 billion proposal for a Bureau of Privacy and Data Security is enacted, Congress will still need to improve upon the *1914 Federal Trade Commission Act*, from which that the FTC draws its authority. Privacy enforcement policies and the rules that govern any new data privacy enforcement office should look to *the Data Protection Act* as a potential model for success.

The Data Protection Act would create new privacy and civil rights authorities to ensure that our regulatory framework can keep pace with the evolving nature of the internet. Our regulations have not kept pace as data collection has grown from simple cookie tracking to extensive surveillance of individuals and communities. Unchecked data practices in many cases reinforce systems of bias that have harmful social, racial, and economic consequences for disadvantaged communities. New and improved data collection techniques, targeted advertising, and automated decision-making are scaling existing bias with harmful practical impacts in areas such as housing, employment, health, education, voting rights, and financial lending. Congress must ensure that there is a civil rights and collective harm mandate as part of any new enforcement authority. *The Data Protection Act* would triple penalties for violations against children, and would essentially function as an improved Children's Online Privacy Protection Act (COPPA) enforcer that would be better equipped to rein in the widespread misuse of children's personal data.

The Data Protection Agency under *the Data Protection Act* also focuses enforcement on the role of data aggregators. A data aggregator is defined within the legislation as any person that collects, uses, or shares an amount of personal data that is not their own and sets the threshold for those entities with an annual revenue of more than \$25 million, or who handles the personal data of 50,000 or more individuals. These aggregators can engage in high risk data practices such as using biometric data for the purposes of uniquely identifying an individual, systemic monitoring of publicly accessible data on a large scale, and sometimes the use of personal data of children or other vulnerable individuals for marketing or profiling purposes. These data practices can lead to negative long term consequences, or privacy harms, for individuals or groups of individuals that have been impacted by the collection or use of their personal data. It will be crucial that privacy enforcement takes a similar tact to regulating data aggregators as *the Data Protection Act*.

Creation of an Independent Data Protection Agency

The Data Protection Agency under *the Data Protection Act* would be an independent agency within the Executive Branch with the sole mandate to regulate high-risk data practices as well as the collection, use, and sharing of personal data. The Director would be appointed to a 5 year term by the President with a subsequent confirmation vote by the Senate. The Director, and their chosen Deputy Director, must possess knowledge and expertise in the areas of technology, protection of personal data, civil rights and liberties, law, and social sciences. The Agency would have the independence and authority to carry out its duties under the *Data Protection Act*, with much of this responsibility designated to the Director. Any new privacy enforcement office must remain independent and be insulated from political influence.

The Data Protection Act establishes three specific units within the Data Protection Agency which should be considered for inclusion in any future enforcement offices: the Office of Civil Rights, the Research Unit, and a Unit to Collect and Track Complaints. The Office of Civil rights

would ensure that the Data Protection Agency itself and the rules it enforces regarding the collection, processing, and sharing of personal data is fair, equitable, and non-discriminatory in treatment and effect. The Office of Civil Rights would work with civil rights advocates, privacy organizations, and data aggregators on the promotion of compliance with civil rights provisions enforced by the Data Protection Agency. The Research Unit proposed by the *Data Protection Act* would be critical to the anticipation of emerging technologies and developing threats to privacy and civil rights. It would be responsible for researching, analyzing, assessing, and reporting on the collection and processing of personal data, including automated decision systems; the collection and processing of personal data by government agencies, including contracts between government agencies and data aggregators; and unfair, deceptive, or discriminatory outcomes that result or are likely to result from the use of automated decision systems, including disparate treatment or disparate impact on the basis of protected class or proxies for protected class. It is important that each individual American has a vector for addressing complaints and seeking recourse. The Unit to Collect and Track Complaints which would function as an office for consumers to file a complaint, to operate a single toll-free telephone number for communication with individuals, a publicly available website, and a publicly available database to facilitate the centralized processing of complaints regarding the collection, processing, and sharing of personal data. These units are important components of the individualized attention and response that should be expected of a modern federal privacy enforcement body.

Congress has a unique opportunity to pass comprehensive data privacy legislation that gives Americans control of their privacy, maintains the United States as a global leader in technology, and preserves democracy in the digital age. The FTC will continue to play an important role in protecting privacy and regulating technology, and it is important for the Senate Committee on Commerce, Science, and Transportation to consider all the tools at its disposal to protect Americans and the innovation that drives our economy. I urge my colleagues to also consider the new tools and missions that are required of our government as technological threats and challenges evolve. *The Data Protection Act* and its establishment of a Data Protection Agency, whose sole mission is to protect our citizen's right to privacy, should be examined as a model from which to build a new privacy enforcement regime for the modern era.

Thank you,



Kirsten Gillibrand
United States Senator

ALBANY/CAPITAL DISTRICT OFFICE ALBANY, NEW YORK REGAN, OFFICE BUILDING 100 SOUTH ALBANY, ALBANY, NY 12207 TEL: (518) 487-2200 FAX: (518) 487-2100	BUFFALO OFFICE 100 EAST TOWN 700 EAST TOWN, BUFFALO, NY 14203 TEL: (716) 855-1200 FAX: (716) 855-1201	LONG ISLAND OFFICE 100 WEST JEFFERSON 100 WEST JEFFERSON, WEST HAVEN, NY 11791 TEL: (516) 865-1200 FAX: (516) 865-1201	NORTH COUNTRY OFFICE PO BOX 25 1000 ALBANY, NY 12212 TEL: (518) 535-1200 FAX: (518) 535-1201	ROCHESTER OFFICE ROCHESTER, NY 14603 1000 ALBANY, NY 14603 TEL: (716) 535-1200 FAX: (716) 535-1201	SYRACUSE/CENTRAL NY OFFICE 100 WEST JEFFERSON, SYRACUSE, NY 13204 100 WEST JEFFERSON, SYRACUSE, NY 13204 TEL: (315) 487-1200 FAX: (315) 487-1201	NEW YORK CITY OFFICE 100 WEST JEFFERSON, NEW YORK, NY 10004 100 WEST JEFFERSON, NEW YORK, NY 10004 TEL: (212) 684-1200 FAX: (212) 684-1201	HUDSON VALLEY OFFICE 100 WEST JEFFERSON, NEW YORK, NY 10004 100 WEST JEFFERSON, NEW YORK, NY 10004 TEL: (914) 684-1200 FAX: (914) 684-1201
---	--	---	---	---	---	---	---

Senator WICKER. Thank you, Madam Chair, and thank you to these witnesses.

The CHAIRWOMAN. Thank you, Senator Wicker, and thank you for that statement. I certainly want to agree with you. Happy to work with a point person from the Administration on this important policy. And I would be remiss if I didn't mention your great work on the European, U.S. data shield discussions. You have been a stalwart on this very important policy issue.

And I think that it shows not only do we have to get our policies right, but that we are in a discussion with the world community about this growing economy as well. So thank you for that. And I very much appreciate your reminding me of your willingness to have a larger discussion about the private right of action. So, anyway, lots to—lots to do here. And so—

Senator WICKER. Thank you.

The CHAIRWOMAN.—I really appreciate those efforts. And so we will now turn to our witnesses. Mr. David Vladeck, Professor and Faculty Director of the Center on Privacy and Technology at Georgetown Law and Former Director of the Federal Trade Commission and Bureau of Consumer Protection. Welcome. Ms. Maureen Ohlhausen—am I saying that right? OK, good.

Ohlhausen, Partner and Section Chair Baker Botts, Former Acting Chairman of the Federal Trade Commission. Mr. Ashkan Soltani, who is joining us remotely, an Independent Researcher and Technologist, but former Chief Technologist for the Federal Trade Commission. And Mr. Morgan Reed, President of The App Association of Washington, D.C. So welcome to all of you. And we will start with you, Professor Vladeck.

**STATEMENT OF DAVID C. VLADECK, PROFESSOR
AND FACULTY DIRECTOR, THE CENTER ON PRIVACY
AND TECHNOLOGY, GEORGETOWN LAW; FORMER DIRECTOR,
FEDERAL TRADE COMMISSION,
BUREAU OF CONSUMER PROTECTION**

Mr. VLADECK. Well, good morning, Chair Cantwell, and Ranking Member Wicker—and I was to say other members of the Committee. I am sure they will file in. I am David Vladeck. I am a Law Professor at Georgetown Law School. And as the Chair mentioned, I am the former Director of the Bureau of Consumer Protection at the Federal Trade Commission. I strongly support the legislation before Congress today. It would provide funding to the FTC to create a new technology center bureau to safeguard your constituents' privacy and data security.

This proposal builds on the Chair's 2019 privacy bill, which also calls for a new technology bureau within the FTC. I support the legislation because it will begin to rectify the chronic underfunding and understaffing of the Federal Trade Commission. It started in 1980s, when the FTC's budget and staff allocations were literally cut in half. Since then, as both—both of you have mentioned, the Nation's gross domestic product has grown exponentially, and the FTC now enforces more than 50 additional laws than it did back in 1980.

But today, the FTC is significantly smaller, both in terms of staffing and funding, than it was in 1980. As best as I can tell, that

is not true for any other Federal agency. And because Federal budgets are based on prior year appropriations, the FTC is still lagging far behind its sister agencies, including, among others, the SEC, the CFPB, and the FCC. But unlike other agencies, the FTC pays for itself. The FTC almost invariably, year after year, returns more money to the Federal treasury than it gets. Why? Because FTC civil penalties, including, for example, the \$5 billion penalty the FTC imposed on Facebook, goes straight to the Treasury.

\$5 billion would pay for more than 15 years of the FTC's budget. If the FTC were a company, we would all want to buy stock in it because it always generates more income than it spends. I urge you to pass this legislation to give the FTC the tools that it needs—desperately needs to fend off and punish privacy violations and other digital harms, from Internet scams and data breaches, to dark pattern manipulation and ransomware attacks. Without more resources, especially more technologists and engineers, the FTC will simply not be able to stem the growing tide of attacks on privacy and other digital harms.

As a result, the cost to the United States will continue to vastly exceed the sums proposed in this legislation. Not enacting this bill would be penny wise and pound foolish. I know that some in this committee think funding and the creation of a new bureau should await Federal privacy legislation. I respectfully disagree. Your constituents are at risk today and that risk grows as privacy averse business models grow. Just read *The Washington Post* today about all of the Internet enabled tools in one's household that are all collecting enormous amounts of sensitive information over which your constituents have little control.

Both of you talked about data breach. Well identity theft is the essentially predictable debris of an Internet economy that doesn't really care about data security. We still are plagued with, you know, with data breaches. So the FTC is really the only privacy cop on the beat. It is time that Congress gave it the tools it really needs to be in this fight. So thank you so much for inviting us here today. I am happy to answer any questions.

[The prepared statement of Mr. Vladeck follows:]

PREPARED STATEMENT OF DAVID C. VLADECK, A.B. CHETTLE, JR. PROFESSOR OF LAW,
GEORGETOWN UNIVERSITY LAW CENTER

Chair Cantwell, Ranking Member Wicker, and members of the Committee, I am David C. Vladeck, a professor at Georgetown University Law Center, former Director of the Federal Trade Commission's Bureau of Consumer Protection, and co-founder and faculty director of Georgetown Law's Center on Privacy & Technology.

I am here to explain why I strongly support the proposed legislation before the Committee today, which will provide funding for the Federal Trade Commission ("FTC") to create a new technology-centered Bureau that will focus on safeguarding your constituents' privacy and data security, and combatting other digital harms. This proposal builds on the Chair's 2019 privacy bill, which called for a new privacy, data security and technology bureau within the FTC.¹

*First, the proposed legislation will ameliorate, but not resolve, the chronic underfunding and under-staffing of the FTC. Even though the United States' gross domestic product ("GDP") has grown at least four-fold since 1980,² and even though the FTC now enforces eighty statutes in addition to the FTC Act, the FTC is signifi-

¹ See Senate Bill No. 2968, 116th Congress, 1st Sess. § 301 (2019).

² See, e.g., <https://www.statista.com/statistics/263601/gross-domestic-product-gdp-per-capita-in-the-united-states/>.

cantly smaller today—in both funding and staffing—than it was in 1980. Passage of this legislation will be an urgently needed boost to the FTC’s ability to fend off and punish privacy violations and other digital harms—from Internet scams and data breaches to dark pattern manipulation and ransom-ware attacks—that threaten businesses, government entities, and your constituents.³

**Second*, the reality is that the FTC does not have adequate resources to safeguard online privacy and fight digital threats, notwithstanding the fact that the FTC remains the most effective enforcement agency in the world. The proposed legislation will help close the resource gap between the FTC and its sister law enforcement agencies. One measure of the resource gap is to compare the FTC’s resources to those of its domestic and international counterparts. In every head-to-head comparison, whether it is with domestic agencies like the Securities and Exchange Commission and the Consumer Financial Protection Bureau, or foreign counterparts like the Irish, British, or French Data Protection authorities, the FTC loses, generally by a wide margin. Without more resources, the FTC will not be able to stem the growing tide of attacks on privacy and other digital harms, and the cost to the United States will continue to vastly exceed the sums proposed in this legislation.

**Third*, the FTC can create a new Bureau to focus on privacy and other digital threats without undermining the Bureau of Consumer Protection’s ability to do its job of protecting consumers in the marketplace. My view (and I emphasize that I am not speaking for the FTC) is that the FTC would benefit from the creation of a new Bureau that would focus on safeguarding privacy and fighting digital harms. The funding authorized in this legislation would allow the FTC to hire and retain a critical mass of technologists, user experience designers, engineers, and other technical staff. The FTC has never had a cohort of technologists, a vacuum that has hindered the Commission’s ability effectively to regulate the major tech companies. To round out a new Bureau, the FTC could transfer the Division of Privacy and Identity Protection (DPIP), which at present has 61 full time employees, almost all lawyers.⁴ The new Bureau would also need to bring in experts from the Divisions of Marketing Practices, Financial Practices and Enforcement, and work closely with other components of the Bureau of Consumer Protection, including the Division of Litigation Technology and Analysis.

My point here is modest: There is plainly a path forward for the FTC to create a new Bureau that focuses on protecting privacy and combatting other digital harms, without undermining the Bureau of Consumer Protection’s ability to do its job. Many senior FTC staff have advocated for the creation of a Bureau to focus on technology-related threats for some time, but given resource constraints, the FTC has been wary about doing so. The enactment of this legislation will give the FTC the tools to reorganize and devote greater resources to fighting digital harms.

I. The FTC Is Under-Funded and Under-Resourced

The FTC’s ever-growing statutory responsibilities, along with the growth of the economy, have long outstripped the Commission’s ability to fully tackle the many missions Congress has assigned to it. This erosion started in the 1980s. Since then, the Commission’s budget and staffing allocations shrank by nearly half. At the same time, the emergence of today’s tech-driven economy has made the FTC’s work far more complex, and issues relating to technology now dominate the Commission’s docket.

Notwithstanding these challenges, the FTC’s domestic and international counterparts are better funded and staffed, especially when measured by their mission and scope. The proposed legislation, if enacted, will begin to address forty years of underfunding and understaffing, and thus help empower the FTC better to protect consumers in the digital age.

The hard fact is that the FTC has never recouped from severe budget and staffing constrictions imposed throughout the 1980s. At its peak in 1980, the FTC had a staff of 1,719 full-time equivalent (“FTE”) employees to enforce approximately thirty statutes.⁵ 1981 marked the beginning of a steady decline in the Commission’s resources. In a seven-year span, the Commission’s budget stalled out at \$66 million,

³See Federal Trade Commission, *FTC Appropriation and Full-Time Equivalent (FTE) History* (last visited Sept. 24, 2021), <https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation>.

⁴FTC, *Fiscal Year 2021 Congressional Budget Justification*, at 121 (available at https://www.ftc.gov/system/files/documents/reports/fy-2021-congressional-budget-justification/fy_2021_cbj_final.pdf).

⁵See Federal Trade Commission, *FTC Appropriation and Full-Time Equivalent (FTE) History* (last visited Sept. 24, 2021), <https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation>.

with its staff whittled down by almost half to a mere 894 FTEs by 1989.⁶ Although there has been some growth in the last decade, the FTC still operated with only a \$331 million budget and only 1,128 FTEs in Fiscal Year 2020 (“FY20”).⁷ This is less than two-thirds of the manpower and only a thirty percent greater budget than the Commission enjoyed forty years ago, yet today’s FTC is charged with a much broader and complex mission than its predecessors. Prior budget increases have been modest, largely covering mandatory increases in staff compensation and infrastructure costs, not desperately needed improvements like hiring technologists and modernizing the Commission’s technology.⁸

While resources have been constrained, the Commission’s responsibilities have expanded and continue to do so. Today’s Commission has the responsibility of enforcing significantly more statutes than it did in 1980. In fact, since 1980, Congress has enacted more than fifty statutes that require the FTC to take action.⁹ The FTC currently enforces eighty-one antitrust and consumer protection laws, as well as the Federal Trade Commission Act.¹⁰ At the end of 2020 alone, three new statutes were enacted tasking the Commission with additional administrative and enforcement duties.¹¹ Not surprisingly, most of the responsibilities Congress has assigned to the Commission relate to privacy and data protection. A number of the post-1980 FTC statutes include important privacy laws such as the Children’s Online Privacy Protection Act (“COPPA”), the Gramm-Leach-Bliley Act, and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (“CAN-SPAM Act”).¹² The FTC’s privacy-related enforcement matters have accounted for more than 130 spam and spyware cases, over 80 cases alleging privacy violations, more than 100 cases under the Fair Credit Reporting Act, and dozens of cases under Gramm-Leach-Bliley, the COPPA, and other related privacy-protective statutes.¹³

Not only have the Commission’s statutory responsibilities expanded, but the U.S. economy has also grown exponentially. In 1980, the U.S. GDP totaled just under \$3 trillion in today’s dollars.¹⁴ Today, it totals about \$21 trillion.¹⁵ And, with the exception of the recession years of 2008 and 2009 and the pandemic year of 2020, the American economy has reliably grown each year.¹⁶ Though we are still in the throes of our battle against COVID-19, both the Federal Reserve and the OECD project a 6 percent GDP growth rate for 2021, thanks in large part to Congressional interventions like the American Rescue Plan.¹⁷

The booming technology sector, where FTC expertise and regulatory oversight are crucial, has contributed much to America’s economic growth since the 1980s. Employment in the technology sector increased by 36 percent from 1990–2000, and by 20 percent from 2010–2015, nearly double total private sector expansion in the same

⁶ See Federal Trade Commission, *FTC Appropriation and Full-Time Equivalent (FTE) History* (last visited Sept. 24, 2021), <https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation>.

⁷ See *id.*

⁸ See Federal Trade Commission, *Prepared Statement Before the Committee on Appropriations, U.S. House of Representatives* (Sept. 25, 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1545285/appropriations_committee_testimony_092519.pdf; Federal Trade Commission, *Fiscal Year 2020 Congressional Budget Justification*, available at https://www.ftc.gov/system/files/documents/reports/fy-2020-congressional-budget-justification/fy_2020_cbj.pdf (requesting budget increase of \$5.98 million, about 73 percent of which would go toward infrastructure improvements and mandatory compensation increases).

⁹ Federal Trade Commission, *Statutes Enforced or Administered by the Commission*, available at <https://www.ftc.gov/enforcement/statutes>.

¹⁰ *Id.*

¹¹ Federal Trade Commission, *Statutes Enforced or Administered by the Commission*, available at <https://www.ftc.gov/enforcement/statutes> (The COVID-19 Consumer Protection Act, the Horseracing Integrity and Safety Act, and the No Surprises Act).

¹² New America, *Revamped FTC or New Agency*, available at <https://www.newamerica.org/oti/reports/does-data-privacy-need-its-own-agency/revamped-ftc-or-new-agency/>.

¹³ Federal Trade Commission, *2020 Privacy and Data Security Update*, (May 24, 2021), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

¹⁴ World Bank, *GDP (current US\$)—United States* (last visited Sept. 23, 2021), <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2020&locations=US&start=1978&view=chart>.

¹⁵ See *id.*

¹⁶ World Bank, *GDP Growth (annual percent)—United States* (last visited Sept. 23, 2021), <https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?end=2020&locations=US&start=1978&view=chart>.

¹⁷ See Organization for Economic Co-Operation and Development, *Keeping the Recovery on Track*, Interim Report (Sept. 2021), <https://doi.org/10.1787/490d4832-en>; Tim Smart, *Fed Holds Steady on Interest Rates but Shaves 2021 Economic Forecast*, U.S. News (Sept. 22, 2021), <https://www.usnews.com/news/economy/articles/2021-09-22/fed-holds-steady-on-interest-rates-but-shaves-2021-economic-forecast>.

window of time.¹⁸ Today, high-tech industries account for about 10 percent of all U.S. jobs and over 18 percent of U.S. output, with growth expected to continue at a faster rate than the overall occupational average.¹⁹

As the tech sector grows, so too does the velocity of the integration of technology into our daily lives, underscoring the need not only for a well-resourced FTC, but for an FTC with specific and deep expertise in technology. The advance of laptops, tablets, smartphones, and other internet-connected devices, along with the near ubiquitous participation in social media, have resulted in the generation of unprecedented amounts of sensitive personal data—including geolocation data, information about political affiliations, product preferences, and attitudes about virtually everything. Much of this personal data is constantly harvested, packaged, and sold and often resold. The commodification of sensitive personal data is a clear threat to consumer privacy and threatens other digital harms.²⁰

To be sure, technologies like videoconferencing have sustained our personal, professional, and academic lives through the pandemic, keeping us connected and “keeping the white-collar economy alive.”²¹ But the FTC’s enforcement action against Zoom underscores that threats to privacy and data security are ever-present, even with what seem to be innocuous technologies.²² The FTC faces a crucial and ever-increasing mission of keeping Americans safe from those who wish to exploit technology for harm or fail to take essential measures to safeguard data. The Committee’s proposal would be a critical first step to ensure the FTC possesses sufficient capabilities to protect consumers as technologies continue to evolve.

II. Comparing the FTC to its Counterpart Agencies Demonstrates the Depth of the Resource Gap

It is hard to showcase the depth of the FTC’s resource deficit in isolation. To drive the point home, consider the asymmetry between the FTC’s mission and budget when compared to Federal agencies with similar, and in some cases narrower, statutory authority. Consider the Securities and Exchange Commission (“SEC”), for example, which oversees securities trading on U.S. equity markets and enforces Federal securities law. To be sure, the SEC has a vital mission to perform, and I am not suggesting that its appropriation is too generous. But the SEC’s annual budget is almost \$2 billion and it has a staff of approximately 4,700 FTEs—that is, nearly six times the FTC’s budget and four times the FTC’s allocation of FTEs.²³ The SEC’s enforcement budget, standing alone, is nearly double that of the entire FTC.²⁴ Even the Consumer Financial Protection Bureau (“CFPB”), which has regulatory authority over certain consumer financial products and services, had a FY21 budget that exceeded the FTC’s budget by almost \$250 million and by nearly four hundred FTEs.²⁵

There is also a significant salary gap between the FTC and other agencies that oversee financial regulation that jeopardizes the FTC’s ability to retain top talent. FTC employees do not qualify for enhanced compensation under the Financial Institutions Reform, Recovery, and Enforcement Act (“FIRREA”). As a result, their salaries are not on par with similarly situated Federal employees working in financial regulation even though the FTC also works on complex investigations of and litigation against the world’s largest corporations.²⁶ And salaries at these corporations

¹⁸ Charles S. Gascon & Evan Karson, *Growth in Tech Sector Returns to Glory Days of the 1990s*, St. Louis Federal Reserve (July 25, 2017), <https://www.stlouisfed.org/publications/regional-economist/second-quarter-2017/growth-in-tech-sector-returns-to-glory-days-of-the-1990s>.

¹⁹ See Brian Roberts & Michael Wolf, *High-Tech Industries: An Analysis of Employment, Wages, and Output*, Bureau of Labor Statistics (May 2018), <https://www.bls.gov/opub/btn/volume-7/high-tech-industries-an-analysis-of-employment-wages-and-output.htm?view=full>; Bureau of Labor Statistics, *Occupational Outlook Handbook: Computer and Information Technology Occupations*, (last visited Sept. 23, 2021), <https://www.bls.gov/ooh/computer-and-information-technology/home.htm>.

²⁰ See Tuan C. Nguyen, *The Brief History of Smartphones*, ThoughtCo (Jan. 30, 2021), <https://www.thoughtco.com/history-of-smartphones-4096585>.

²¹ See Matthew Yglesias, *The Tech Sector is Finally Delivering On Its Promise*, Vox (Apr. 7, 2020), <https://www.vox.com/2020/4/7/21209605/solow-paradox-coronavirus-technology>.

²² See FTC, *In the Matter of Zoom Video Communications, Inc.*, <https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf>.

²³ See Securities and Exchange Commission, *Fiscal Year 2022 Congressional Budget Justification and Annual Performance Plan and Fiscal Year 2020 Annual Performance Report 2* (2021), available at <https://www.sec.gov/cj>.

²⁴ *Id.* at 23.

²⁵ Bureau Of Consumer Financial Protection, *Annual Performance Plan and Report*, and *Budget Overview 10* (2021), available at https://files.consumerfinance.gov/f/documents/cfpb_performance-plan-and-report_fy21.pdf.

²⁶ Paul H. Kupiec, *The Money in Banking: Comparing Salaries of Bank and Bank Regulatory Employees*, American Enterprise Institute for Public Policy Research 7–10 (April 2014).

and the law firms that represent them dwarf those in government, which has helped tech giants, like Google, Facebook, Amazon and others, poach FTC staffers at a remarkable rate.²⁷ Leveling FTC employees' salaries with their government counterparts would restore parity within government and help the FTC retain top talent, including technologists and engineers.

The FTC's resources also pale in comparison to its international counterparts. Many of our European allies have created agencies to enforce privacy and data security protections—just a part of what the FTC does.²⁸ For example, Ireland's Data Protection Commission ("DPC") has 145 staff members, for a nation with a population around 5 million.²⁹ DPC Commissioner Helen Dixon said these resources are "vital for the DPC to continue to build its capacity as an internationally respected and effective supervisory authority."³⁰ If the FTC had comparable staff proportional to the U.S. population of over 333 million, it would have over 9,600 staff dedicated just to privacy. The British Information Commissioner's Office ("OIC") has more than 500 staff members.³¹ France's data protection authority ("CNIL") has 255 staff members to protect a population of about 65 million, and it is backed up by its sister agency, Inria (the French National Institute for Research in Digital Science and Technology), which has nearly 4,000 engineers on staff.³² That's a drastic difference given only 61 FTC staffers are dedicated to protecting the privacy of more than 333 million Americans. The resources of our foreign counterparts continue to grow in proportion to the need for privacy regulations while the FTC's resources remain static.

Increasing the FTC's budget is absolutely necessary. Even with its limited funding and staffing, the FTC continues to operate at a high level, as demonstrated by its recent order enforcement case against Facebook, which resulted in the strictest consent decree ever entered anywhere, as well as a record-breaking \$5 billion penalty, and a steady stream of enforcement cases. But meeting the challenges of protecting consumers from privacy violations, data breaches, identity theft, and other digital harms requires an infusion of funding and staff. The FY22 President's budget proposal is insufficient; its increase to \$389 million and 1,250 FTEs is a start, but still wholly inadequate. On the other hand, the proposed infusion of \$1 billion for a new Bureau that focuses on digital privacy and cybersecurity can be a game-changer. I support this proposal because it will align the FTC's budget with the realities of today's tech-based economy, help restore the FTC to parity with its domestic and international counterparts, and better enable the FTC to perform its important mission of protecting consumers.

III. Funding Will Enable the FTC to Create a Bureau Focusing on Fighting Digital Harms

There is no question that if Congress enacts the pending legislative proposal the FTC will be able to create a new Bureau devoted to fighting against digital harms without hollowing out the Bureau of Consumer Protection ("BCP"). After all, there is plenty of work for a new Bureau to focus on technology and digital harms and BCP will still have an avalanche of consumer protection work to keep it fully engaged. I recognize that for government veterans, the word "reorganization" is justifiably greeted with skepticism, alarm, or worse. But there is a difference where, as would be the case here, reorganization takes the form of adding substantial resources rather than simply re-allocating existing resources.

In my view, the first and most important measure the FTC should take in standing up a new Bureau is to recruit and hire a critical mass of top-notch technologists. As far as I know, the FTC has never been able to have more than ten technologists on staff at any given time (and probably far fewer), and the small cohort has made it difficult for the FTC to retain technologists. The FTC likely needs several multiples of ten to ensure that the FTC has the expertise to regulate the major tech

²⁷ See Alex Kantrowitz, "It's Ridiculous." *Underfunded FTC and DOJ Can't Keep Fighting the Tech Giants Like This*, Big Technology Newsletter (Sep. 17, 2020), <https://bigtechnology.substack.com/p/its-ridiculous-underfunded-us-regulators>.

²⁸ The GDPR explicitly requires that the member states' Data Protection Supervisory Authorities be provided with the financial and human resources, premises, and infrastructure necessary for the effective performance of their tasks. Commission Regulation 2016/679, General Data Protection Regulation, art. 1, 2016 O.J. (L 119) 1, 22.

²⁹ <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2020-annual-report>; <https://www.dataprotection.ie/sites/default/files/uploads/2021-05/DPC%202020%20Annual%20Report%20%28English%29.pdf>

³⁰ <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-funding-2021-budget>.

³¹ <https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/>.

³² https://www.cnil.fr/sites/default/files/atoms/files/the_cn timer_in_a_nutshell_2021.pdf. See also <https://www.inria.fr/en/inria-ecosystem>.

companies. And a critical mass of technologists is essential for several reasons, including instilling camaraderie and information sharing, enabling the Bureau to engage in multiple investigations simultaneously, helping staff with Section 6(b)³³ investigations, and giving the technologists time to keep up with emerging technologies and to conduct and publish research.³⁴

To fully staff the new Bureau, the 61 staff currently assigned to BCP's Division of Privacy and Identity Protection would be transferred to the new Bureau. The new Bureau would also need to recruit a few experienced lawyers from several BCP Divisions, including Marketing Practices, Financial Practices, Enforcement, and Litigation Technology and Analysis. I assume that those Division would be able to replace lost staff.

A fully staffed new Bureau could also make critical changes to the way the FTC enforces the law. For one thing, the new Bureau could engage in real-time oversight of the tech companies to understand what they are actually doing in the marketplace, enabling the new Bureau of be pro-active in ways the FTC cannot undertake today. For another, having an in-house complement of technologists would enable the FTC to undertake simultaneously multiple investigations that require technical assistance, especially in investigations into data breaches, spyware, the Internet of Things, and the misuse of personal information. For yet another, the new Bureau could take over the responsibility of monitoring existing consent decrees involving tech companies, to ensure that the companies adhere to the requirements of the decrees, and if there are defaults, to help decide whether the FTC should launch an investigation or pursue an enforcement action.

And last, but hardly least, the new Bureau will have the authority, subject to Commission approval, to significantly modify the FTC's orders against tech companies. Due to resource constraints, FTC privacy orders require the company to hire a third-party assessor to conduct periodic audits. Section VIII of the FTC's 2019 Order Modifying Prior Decision and Order for Facebook lays out what is now the standard practice of requiring the company to hire an assessor, subject to the FTC's approval, to submit an initial assessment within six months, and thereafter submit biennial assessments.³⁵ But the FTC adopted the practice of using outside assessors in privacy cases mainly because of the resource constraints I have catalogued above. The new Bureau may choose to play a far more active, direct role in overseeing tech companies subject to FTC orders, and may, for example, require more frequent and robust exchanges between the FTC and the company so the FTC, in real-time, can assess whether the company is in fact in compliance with the FTC's order.³⁶

* * *

Let me end by making a few additional points that are not part of the pending legislation but are issues Congress must tackle if the FTC is going to fulfill its mission of safeguarding consumer privacy.

First, the FTC needs ordinary notice and comment rulemaking authority under Section 553 of the Administrative Procedure Act; without it, the FTC has no choice but to make policy through enforcement cases, a process that is slow, resource-intensive, and does not necessarily yield clear-cut standards.³⁷

³³ 15 U.S.C. 46(b).

³⁴ Having in-house experts would substantially bolster the effectiveness of the FTC's enforcement cases, regardless of whether the cases are brought before the Administrative Law Judge or a Federal court. For instance, in *FTC v. Commerce Planet*, a case that spanned 18 trial days, the FTC retained an expert on human computer interaction (in other words, user experience) to testify that the company's disclosures were designed to be obscured and were misleading. In ruling for the FTC, the District Court Judge said that "the Court finds the expert testimony of Jennifer King to be on-point and persuasive," sealing the FTC's win. *FTC v. Commerce Planet*, 878 F. Supp. 2d 1048, 1068 (C.D. Cal. 2012), *aff'd*, 815 F.3d 593 (9th Cir. 2016). Because of the expense of hiring outside experts, the FTC rarely does so in consumer protection cases.

³⁵ <https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf>.

³⁶ I should acknowledge that I was the Director of the FTC's Bureau of Consumer Protection when the Commission was crafting the initial orders in the Facebook and Google cases. Because of resource constraints, there was no discussion that the FTC should take on the front-line role of assessing the companies' ongoing compliance with the orders. For that reason, the FTC relied on third-party independent assessments; the utility of those assessments is subject to debate. There is no question that the assessments have worked reasonably well in the seventy or so data breach cases the FTC has brought.

³⁷ I recently testified in favor of House Bill 4447 before the House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, which would restore to the FTC notice and comment rulemaking authority. See https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/WitnessTestimony_Vladeck_CPC_2021.07.28.pdf.

Second, the FTC needs initial fining authority, especially in cases involving digital harms. Companies should not get a free pass on privacy violations. Under existing law, however, the only remedy for a first violation is a consent order, not a fine, and not redress, not just because of the Supreme Court's ruling in *AMG v. FTC*, but because the currency in privacy violations is the misuse of sensitive personal data, which, unlike money, cannot be refunded or restored.

Third, the statutory tools the FTC has available are not sufficient to provide robust protection for consumers against digital harms, including privacy harms. The commands of Section 5 the FTC Act—that the FTC “prevent” “unfair and deceptive practices” in the marketplace—are not, in themselves, sufficient to create a meaningful legal regime that safeguards consumers. To be sure, the Act provides substantial ammunition for the Commission to bring enforcement cases for many kinds of egregious privacy harms; ammunition that the Commission has used against most of the major technology companies. But Section 5 cannot restrain more insidious practices that go beyond unfairness and deception, and Congress needs to enact a comprehensive privacy law or delegate greater power to the FTC to combat digital harms.³⁸

The CHAIRWOMAN. Thank you, Professor Vladeck. Ms. Ohlhausen, thank you for being here.

**STATEMENT OF MAUREEN K. OHLHAUSEN, PARTNER AND
SECTION CHAIR OF ANTITRUST AND COMPETITION LAW,
BAKER BOTTS; FORMER ACTING CHAIRMAN, FEDERAL
TRADE COMMISSION**

Ms. OHLHAUSEN. Thank you. Thank you, Chairman Cantwell, and Ranking Member Wicker, and the other distinguished members of this Committee for the opportunity to testify at this important hearing examining how to protect consumer privacy. As you have already noted, I am Maureen Ohlhausen. I am a Partner at the law firm of Baker Botts, and I also had the pleasure of serving as an Acting Chairman and Commissioner at the Federal Trade Commission, our Nation's leading consumer protection agency.

As the collection, use, and sharing of personal data has continued to grow, the FTC is reaching the limits of its current tools, and consumers and businesses are increasingly required to navigate a tangle of confusing and often inconsistent privacy requirements from various levels of Government. And to safeguard consumer privacy in today's environment, Congress needs to enact a comprehensive national privacy law. And that is why it is paramount that members of this committee return to the bipartisan negotiations conducted in the previous Congress. A new law should have several components.

First, legislation should provide consumers clarity and visibility into companies' data collection use and sharing practices, as well as choices regarding these practices calibrated to the sensitivity of that data. Second, legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. Third, it should ensure strong enforcement that protects consumers from harmful data practices while allowing companies to provide innovative products and services that consumers want. And while though some have raised the possibility of the FTC undertaking a privacy rulemaking under its current general unfair and deceptive authority, I am concerned that a potential FTC pri-

³⁸I would like to acknowledge the exceptional assistance in preparing this testimony provided by Georgetown Law Center's Communications and Technology Law clinic, including the clinic's director, Professor Laura Moy, staff attorneys Victoria Tang and Daniel Jellins, and students Liliana Fiorenti, Anna Butel, Pariss Briggs and Philip Robins.

vacy rulemaking may actually distract from focusing on achieving these key objectives through legislation.

And there are several potential problems with an FTC rulemaking. First, the scope of an FTC rulemaking under the agency's current UDAP authority is much more limited than what Congress can achieve statutorily. For example, the requirement of access and correction rights for consumers, which we have seen in a number of proposed bills, is likely not supportable under the FTC's current general authority. And some of my fellow panelists have acknowledged the limitations of the FTC's current authority in their testimony.

Second, an FTC rulemaking may not preempt State laws and regulations, even conflicting State requirements. Thus, an FTC rulemaking could simply produce a 50 first set of privacy requirements rather than a single national framework that applies no matter where consumers live, work, shop, or visit. And this would lead to even more consumer and business confusion and a fragmenting of consumer rights. And it would also be particularly burdensome on smaller firms that lack the resources to deal with such regulatory complexity.

Third, Congress put significant limitations in place for FTC UDAP rulemaking absent specific guidance to the contrary. And where Congress has enacted specific privacy laws such as in the areas of children's privacy and credit reporting, it has given the FTC notice and comment APA rulemaking authority to implement clear statutory direction. Absent such clear statutory guidance and streamlined rulemaking authority, the FTC must proceed under the more deliberate Magnuson Moss process, which will slow the implementation of consumer protections that are widely supported by Congress.

Now, there is no question that a strong privacy law needs to include strong FTC authority to protect consumers' rights. A single Federal privacy law that gives the FTC more enforcement authority will dramatically strengthen consumer protections. And it should authorize the FTC to fine companies for certain first time violations, and in certain cases to issue rules to keep up with developments in technology. It should also give the FTC more resources. State AGs should be given the power to enforce any new Federal law. And a consumer privacy law, though, should not include private rights of action with punitive or statutory damages that would primarily benefit lawyers and result in class actions that provide little, if any, relief to actual victims.

Giving the FTC specific authority to provide consumer redress would be an effective way to enable consumers to be compensated directly and promptly when companies engage in harmful data practices. So thank you again for the opportunity to testify today, and I look forward to working with the Committee and all stakeholders to craft strong national privacy legislation.

[The prepared statement of Ms. Ohlhausen follows:]

PREPARED STATEMENT OF MAUREEN K. OHLHAUSEN, FORMER ACTING CHAIR,
FEDERAL TRADE COMMISSION

Chair Cantwell, Ranking Member Wicker, and other distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing

examining how to better protect consumer privacy. My name is Maureen Ohlhausen, and I am a partner at the law firm Baker Botts L.L.P. I had the pleasure of serving as an FTC Commissioner (2012–2018) and Acting Chairman (2017–2018).

The FTC is our Nation's leading consumer privacy protection agency. It has brought hundreds of privacy and data security-related enforcement actions, covering both on- and offline practices and fast-evolving technologies.¹ The FTC has creatively used every enforcement, policy, and educational tool at its disposal in its privacy and data security work to protect consumers' personal information, while still allowing consumers to enjoy the benefits of the many innovative products offered in today's dynamic marketplace. However, as the collection, use, and sharing of personal data have continued to grow in amount and complexity, consumers and businesses are now required to navigate a tangled web of confusing, and often inconsistent, data privacy requirements from various levels of government, and from various nations and regions throughout the world.

While I am proud of the FTC's privacy and data security enforcement efforts, the agency currently operates under several material constraints that limit the FTC's effectiveness absent further action by Congress. You and your colleagues can remove these constraints by enacting comprehensive, technology neutral, national privacy legislation that provides clear protections for consumers, articulates specific limits on companies' ability to collect, use, and share sensitive personal information, and grants the FTC the resources and explicit authority necessary to enforce a new law.

I would like to address what I view as reasons why reliance on the FTC's current authority cannot provide the same benefits as a Federal privacy law. First, with the exception of discrete areas such as children's privacy and fair credit reporting, the FTC lacks explicit authority to enforce statutory privacy requirements or promulgate privacy regulations. Section 5 of the FTC Act gives the agency the authority to prevent certain entities from "using . . . unfair or deceptive acts or practices in or affecting commerce" ("UDAP"). This language has rightly been interpreted to permit the FTC to police unfair or deceptive privacy and data security practices, but it does not provide the clear statutory guidance found in other laws. For example, under the Fair Credit Reporting Act, the FTC can impose affirmative obligations on entities to provide rights of access to and correction of data. These rights would also be available under Federal privacy legislation introduced by Members of this Committee. But the FTC likely could not impose such obligations based on its UDAP authority alone.

Second, the FTC's ability to promulgate rules under its broad UDAP authority is governed by a special process in the Magnuson-Moss Warranty-Federal Trade Commission Improvement Act. Congress set up this process specifically to cabin the agency's broad UDAP authority by imposing additional procedural requirements and other protections.² By contrast, where Congress has provided the agency with detailed statutory guidance on subject matter and goals, it has expressly permitted the FTC to use Administrative Procedure Act notice-and-comment rulemaking, and specifically exempted the agency from the additional procedures of Magnuson-Moss rulemaking.

Third, an FTC rulemaking under existing authority may not necessarily preempt state laws. If the FTC does not preempt state laws, this would permit the continued proliferation of disparate state requirements, and would make a coherent, consistent national framework nearly impossible. In addition, there will inevitably be a conflict between an FTC rulemaking and the increasing number of state laws and rulemakings, which will create confusion with respect to what requirements apply, and will further fragment U.S. privacy protections.

Simply put, the FTC's existing framework is not conducive to adopting comprehensive, national consumer privacy and data security requirements in a manner that can provide the clarity and certainty consumers and businesses seek. That is why I respectfully request that Congress turn its focus back to enacting privacy legislation.

¹See, e.g., FED. TRADE COMM'N, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY (2020), <https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf>; *Oversight of the Federal Trade Commission: Strengthening Protections for American's Privacy and Data Security: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 116th Congress (2019–2020) (statement of the FTC), https://www.ftc.gov/system/files/documents/public_statements/1578963/p180101testimonyftcoverisight20200805.pdf.

²Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93–637, §202, 88 Stat. 2183, 2193 (1975) (codified as amended at 15 U.S.C. §§45–46, 49–52, 56–57c, 2301–2312 (2012)); 15 U.S.C. §57a(a)(1)(B).

Last year, I testified before this committee in support of Congressional efforts to enact comprehensive Federal privacy legislation. The events of the past year make the need for such legislation even more apparent. Due to the COVID-19 pandemic, we have seen a rapid shift to online work and learning, as well as the deployment of technological efforts to track the path of the virus. The California Consumer Privacy Act (“CCPA”) went into effect in 2020, but the landscape continues to shift, as California’s ballot initiative (the California Privacy Rights Act) amended the CCPA, and Virginia and Colorado enacted their own consumer privacy laws.

These developments reinforce the need for Federal action. Congress needs to act quickly, and I urge the Leadership and Members of this Committee to continue to take important steps in that direction.

I realize that there are still points of contention with respect to privacy legislation. However, what we all have in common is a desire for clear consumer privacy protections that apply throughout the Nation based on the sensitivity of the data, and which allow consumers to continue to benefit from innovative technologies, such as those we have come to rely on even more heavily during this pandemic. We want consumers to enjoy confidence that their personal information is not subject to varying protections within a state or from state to state, regardless of the entity that collects such information, based on the sensitivity of the data and how it is used.³

I support strong consumer privacy rights and believe firmly in providing transparency and control to consumers, robust security, and strong accountability as outlined in the FTC’s bipartisan 2012 landmark Privacy Report.⁴ Further, as someone who has also focused on the intersection of antitrust and privacy law, and the impact of regulation of market competition, I urge that a federal approach be technology-neutral and avoid unduly burdening smaller entities, innovative services, or certain entities in the Internet ecosystem.

Key Elements of an Effective Federal Framework

I strongly believe that Congress needs to enact Federal privacy legislation that includes several key attributes. First, legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. Second, it should ensure strong enforcement that protects consumer information that could result in harm if disclosed or misused, while also allowing companies to provide and develop innovative products and services that consumers want. Third, it should provide consumers clarity and visibility into companies’ data collection, use, and sharing practices, as well as easily understandable choices regarding these practices, calibrated to the sensitivity of that data. Fourth, legislation should be more comprehensive than current state laws, such as the CCPA, addressing more elements of the data cycle. Fifth, Federal privacy legislation should be enforced by the FTC, which has the experience and skill to meaningfully enforce a new law’s protections, supplemented by state attorneys general (“AGs”).

1. Provide a national and uniform set of protections and consumer rights

Federal legislation should be technology-neutral and apply to all entities across the Internet ecosystem that collect, share, or make use of consumer data, whether they are technology companies, broadband providers, or retailers. What matters is not who collects the data, but what data is collected, how sensitive it is, and how it is protected and used.

Strong privacy protections need to apply to consumers regardless of where in the United States they live, work, or happen to be accessing information. By its very nature, the Internet connects individuals across state lines. Data (and, increasingly, commerce) knows no state boundaries. For this reason, a proliferation of different state privacy requirements creates inconsistent and confusing privacy protections

³See Memorandum from Public Opinion Strategies and Peter D. Hart to the Progressive Policy Institute, Key Findings from Recent National Survey of Internet Users (May 26, 2016), <https://www.progressivepolicy.org/wp-content/uploads/2016/05/Internet-User-National-Survey-May-23-25-Key-Findings-Memo.pdf> (finding that 94 percent of consumers favor such a consistent and technology-neutral privacy regime, and that 83 percent of consumers say their online privacy should be protected based on the sensitivity of their online data, rather than by the type of Internet company that uses their data). See also <https://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rulesprotecting-information/> (“Ultimately, consumers want to know there is one set of rules that equally applies to every company that is able to obtain and share their data, whether it be search engines, social networks, or ISPs, and they want that data protected based on the sensitivity of what is being collected” said Peter Hart.”).

⁴See FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

for consumers, as well as significant compliance and operational challenges for businesses of all sizes. Although privacy regulation is often justified by concerns about big online players having large amounts of consumer information, regulatory complexity actually works to favor large, established companies.⁵ It also erects barriers to the kind of innovation and investment that is a lifeblood of our Nation's economy and to many beneficial and consumer-friendly uses of information.

2. Protect consumer information that could result in harm if disclosed or misused

A Federal privacy law should protect individuals' information, the use or disclosure of which could result in harm. Accordingly, such legislation should cover data that identifies an individual, whereas data that does not identify an individual poses a minimal risk of harm and need not be subject to the same requirements.

Sensitive personal information, such as health and financial information, real-time precise geo-location information, social security numbers, and children's information, poses the highest risk of consumer harm and should be subject to the highest protections.⁶ In turn, to mirror consumer expectations and preferences, there should be less-stringent requirements on non-sensitive personally identifiable information, reflecting the lower risk of consumer harm. Information that is reasonably de-identified, aggregated, or publicly available does not raise the same specter of harm and falls outside the scope of necessary consumer protections.

3. Reflect consumer preferences through simple choices based on data sensitivity

I believe that an optimal approach would balance ease of use and transparency by giving consumers clear and simple privacy choices based on the nature of the relevant information itself—its sensitivity and the correlated risk of consumer harm if such information is the subject of an unauthorized disclosure. A Federal privacy law should promote consumer control and choice by imposing requirements for obtaining meaningful consent based on the risks associated with different kinds and uses of consumer data.

As I discussed earlier, sensitive data should be afforded stronger protections under a Federal privacy law than non-sensitive personally identifiable data and non-identifiable information. In line with this concept, the most sensitive data should be subject to an opt-in consent requirement, while other personally identifiable covered data would be suitably protected by opt-out consent. Further, for certain types of routine operational uses, such as order fulfillment, fraud prevention, network management, and some forms of first-party marketing, consent should be inferred, consistent with consumer expectations.

4. Legislation should be more comprehensive than current state laws

Federal privacy legislation should address gaps and shortcomings of current privacy laws. A strong Federal privacy law should build on elements of current efforts in California, Virginia, and Colorado, and include safeguards protecting uses of consumer data throughout the United States.

5. Ensure strong accountability and enforcement that best protects consumer interests

The Members of this Committee recognize that Congress must develop a law that guarantees strong privacy rights to consumers and adopts best practices from state laws, while creating uniformity across the Nation. But preempting state laws should not mean weakening protections for consumers. A Federal privacy law needs to be a strong one. I believe that states, as well as the FTC, have a critical role to play in protecting and enforcing those rights.

The FTC should have the primary authority to enforce a national privacy law. The FTC is already protecting consumer privacy, making it experienced and knowledgeable in the field. Moreover, it is well-equipped to assess the interaction between competition and privacy law in the United States. Congress should make use of these existing strengths, rather than start from scratch with a newly-formed, and inexperienced, agency.

Federal privacy legislation should support strong enforcement by the FTC, allowing the agency to obtain meaningful results. Rather than being limited to violations of previous orders, the FTC needs to be able to fine companies for first-time violations of a new, comprehensive privacy law to provide sufficient incentives for compa-

⁵ See, e.g., Jian Jia, Ginger Zhe Jin, Liad Wagman, "The Short-Run Effects of GDPR on Technology Venture Investment" (working paper, National Bureau of Economic Research, November 2018), <https://www.nber.org/papers/w25248>.

⁶ These types of information reflect a general consensus, as recognized in the FTC's 2012 report, *supra* note 4 at 58–59. Other types of information may be sensitive, as reflected in consumer expectations.

nies to take the necessary steps to ensure responsible use and protection of consumer data.

However, as I discussed earlier, as privacy concerns become weightier and more complex, the FTC is reaching the limits of its current tools—which it has made clear in its statements, including those made before the Committee.⁷ Congress must provide the FTC with greater statutory clarity coupled with more resources to protect consumer privacy in America.

Despite the ever-growing need for privacy enforcement, the FTC’s budget has been flat since 2013. The number of full-time employees lags behind where it was in the early 1980s and comparable bodies tasked with data protection.⁸ Meanwhile, the Internet and the collection, use, and sharing of consumer data have grown enormously. I urge Congress to address that widening gap to meaningfully support an issue as important and complicated as consumer privacy.

I recognize that state AGs are critical allies in the realm of consumer protection. They should be given the power to enforce any new Federal law, taking on violations that the FTC is yet to investigate or that have a particular impact in their respective state. By working in unison, the FTC and state AGs can create an efficient process that reduces duplicative matters and supports consistency for all consumers.

A Federal privacy law, though, should not include private rights of action with statutory or punitive damages. These approaches often result in class actions that primarily benefit attorneys, while providing little, if any, relief to those who are harmed. Private rights of action may also lead to abuses, such as frivolous assertions and attempts to seek “nuisance fee” settlements. This results in the diversion of company resources from compliance to litigation, which ultimately does not help consumers who, at the end of the day, simply want companies to follow the law. Like state law preemption, trusting enforcement to the FTC and state AGs fosters consistency, and is ultimately more beneficial to consumers.

Providing the FTC and state AGs with clear privacy protections, backed up with strong enforcement authority and expanded resources, represents a highly beneficial approach for consumers, as evidenced by the successful and bipartisan work in policing violations of children’s privacy through the Children’s Online Privacy Protection Act. Providing the FTC with enhanced authority to facilitate consumer redress for privacy violations would also ensure that consumers can be compensated directly and promptly when companies engage in harmful data practices.

Conclusion

Thank you again for the opportunity to testify today. I look forward to working with all Members of the Committee and all stakeholders in crafting strong national privacy legislation.

The CHAIRWOMAN. Thank you very much, Ms. Ohlhausen. Now we are going to hear remotely from Mr. Ashkan Soltani, Independent Researcher and Technologist, former Chief of the Federal Trade Commission.

STATEMENT OF ASHKAN SOLTANI, INDEPENDENT RESEARCHER AND TECHNOLOGIST; FORMER CHIEF TECHNOLOGIST, FEDERAL TRADE COMMISSION

Mr. SOLTANI. Hello there. Can you hear me alright?

The CHAIRWOMAN. Yes.

Mr. SOLTANI. Perfect. Chair Cantwell, Ranking Member Wicker, and members of this committee, thank you for inviting me to appear today. My name is Ashkan Soltani. I am a researcher and technologist, formerly Chief Technologist at the FTC. Since departing FTC, I have helped support State level privacy and tech enforcement, both as an expert and through my involvement through

⁷ See, e.g., FED. TRADE COMM’N, FTC REPORT ON RESOURCES USED AND NEEDED FOR PROTECTING CONSUMER PRIVACY AND SECURITY (2020), <https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf>; *Oversight of the Federal Trade Commission*, *supra* note 1 at (“Section 5, which we use to bring our general privacy and data security cases, is not without its limitations.”).

⁸ *Id.* at 2–3.

Georgetown law, where I am a distinguished fellow at the Institute of Law and Policy and the Center of Privacy and Technology.

I also helped author California's landmark privacy laws, the CCPA and the CPRA, Prop 24 which California voters enthusiastically passed last year. I have seen firsthand the challenges of crafting and enforcing laws that constrain bad behavior in the current digital ecosystem. I am pleased to be invited as Congress and this committee are considering significant changes to the structure and funding of the FTC. The proposal to create and fund a new bureau at the FTC is a strong step forward and providing the Commission with the resources it needs desperately to effectively protect consumers in the digital economy.

A new bureau focused on technology and data protection would help the FTC support its mission of policing unfair and deceptive trade practices related to privacy, data security, identity theft, and data abuses. I have submitted my written testimony for the record, but I would like to highlight three key points which I hope will inform the discussion today. One is that the FTC is critically under-resourced to oversee the Nation's myriad of privacy and cybersecurity issues. With a bare bones staff of about 40 attorneys and a handful of technologists, their researchers pale in contrast to their counterparts in other countries.

The German DPA, for example, has 745 staff and nearly 100 tech experts enforcing their laws for a country one-quarter of the population in the US. Similarly, France, which has one-fifth of our population employs nearly 200 staff, including 30 tech experts. The research problem is exasperated when businesses choose to litigate a case rather than accept a settlement. By some accounts, litigation can occupy one-third to one-half of the Commission's entire privacy division on a single matter. That is the entire Federal—that is half of the entire Federal privacy staff working on one case for years at the exclusion of other critical work.

Similarly, the FTC Bureau of Enforcement is tasked with overseeing compliance with all of the hundreds of FTC consent decrees, in addition to a myriad of obscure laws relating to, for example, Made in the USA and textile labeling. The same lawyers who ensure that social media companies have robust privacy and data security programs are also making sure the labels on bed linens are correct. In fact, many of the big tech companies which this Congress is presently concerned with, such as Facebook, Apple, Google and others, are already under a consent decree with the Commission.

But the FTC has limited resources to adequately monitor that these firms are complying with the terms of their order. One former FTC enforcement staff has publicly stated the FTC rarely even reads the third party assessments provided to it. Additionally, the FTC doesn't need just more resources. It needs the right resources. Technology and data provides—pervades nearly every aspect of today's online marketplace. Data security, data abuse, identity theft all have one thing in common, technology and the underlying data they rely on.

Narrowly constraining the new bureau to solve only one of those problems, privacy, would fall short of the consumer protection goals laid out by FTC and this Congress. I suggest instead Congress sup-

port the creation of the Bureau of Technology and Data Protection. This may seem like a small point, but names do matter. As I said before, most harms don't concern just privacy but data, data abuse. I have long advocated for the creation of a new Bureau of Technology with the mission and expertise to investigate harmful practices across the technology ecosystem.

This new bureau would provide a hub of resources that would serve across the agency's many consumer protection missions, incentivize collaborations, and encourage efficiency, similar to how BE functions across division. Alongside the funding, Congress should take steps to ensure that the Commission hires a wide range of staff to this bureau outside of just traditional lawyers, economists, and even technologists like myself. Importantly, the agency should hire statisticians, UX designers, social scientists, and behavioral researchers such as experts in child development who can guide the complex cases that come before them across a myriad of technology issues, such as dark patterns, and manipulative design, and algorithmic discrimination.

Finally, in addition to more resources, I support my panelist's call that the FTC needs additional legal authority to meet the challenges of the digital economy. By expanding the Commission's budget is a great first step, this Congress should complement that funding with additional privacy authority so that the agency can fulfill its mission. This is why it is critical that this Congress pass Federal privacy legislation that builds upon but does not preempt privacy legislation adopted in states like California and Colorado.

I am happy to go into what attributes of such legislation should look like, but based on my experience in California, the most critical is the ability to allow experimentation in the states as we seek to find the appropriate approach to the complexities of the digital ecosystem. Thank you for the opportunity to testify today. I am excited to work with you all on helping to solve these challenges.

[The prepared statement of Mr. Soltani follows:]

PREPARED STATEMENT OF ASHKAN SOLTANI, INDEPENDENT RESEARCHER AND TECHNOLOGIST; FORMER CHIEF TECHNOLOGIST, FEDERAL TRADE COMMISSION

Dear Chair Cantwell, Ranking Member Wicker, and Members of the Committee:

Thank you for inviting me here today to testify before you. My name is Ashkan Soltani. I am a researcher and technologist, and formerly served as the Chief Technologist at the Federal Trade Commission (FTC or Commission).

Since departing the FTC, I've helped support state-level privacy and tech enforcement, both directly as an expert, and through my involvement with Georgetown Law, where I am a Distinguished Fellow at both the Institute for Technology Law & Policy and the Center on Privacy and Technology. I also helped author California's landmark privacy laws, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). I have seen firsthand the challenges in bringing cases against technology companies and making new laws to constrain bad behavior.

Today, I'd like to discuss why the FTC needs expanded authority to handle data and technology matters, how to appropriately expand the Commission's staff and talent pool, and why it is important that any new bureau have a specific mandate to investigate new technologies and harmful data practices that pervade the modern digital ecosystem.

Expanding FTC Authority

I'm pleased to be invited as Congress and this Committee are considering significant changes to the structure and funding of the Federal Trade Commission. The proposal to create and fund a new bureau at the FTC—which Chair Cantwell also

called for in S. 2968, the Consumer Privacy Rights Act—is a strong step forward towards providing the Commission with the resources it needs to effectively protect consumers in the digital economy. A new bureau focused on technology and data protection would help the FTC support its mission of policing unfair and deceptive practices related to privacy, data security, identity theft, and data abuses. I strongly support it.

First and foremost, in addition to more resources, the agency desperately needs additional legal authority to meet the new challenges of the digital economy. With the exception of a few sectoral laws, such as the Children’s Online Privacy Protection Act (COPPA) or the Fair Credit Reporting Act (FCRA) there is no comprehensive Federal privacy regime in the United States. We’re long overdue for a change.

Many of the digital harms from the surveillance economy are monitored through the FTC’s enforcement of deceptive practices under Section 5 of the FTC Act. But this framework does not effectively protect consumers. For example, consumers often don’t directly interact with the hundreds of data brokers that surreptitiously collect their data as they move about their digital lives. This ecosystem makes the required “notice” component of a deception case difficult to prove. Unfairness authority is hard to use to enforce privacy harms, since the courts have not typically recognized privacy harms as cognizable injuries under FTC unfairness standards. Moreover, the FTC lacks the authority to issue civil penalties for first-time violations.

While expanding the Commission’s budget is a great step, Congress should complement that funding with additional privacy authority so the agency can properly fulfill its mission. That’s why it is critical that Congress passes Federal privacy legislation that builds upon, but does not preempt, privacy legislation adopted in states like California and Colorado. Already, there has been a concerted effort in Congress and in statehouses across the Nation to muddy the conversation and introduce privacy bills that appear strong, but merely entrench the status quo of privacy violations. Specifically, bills like the one adopted in Virginia appear robust, but allow exploitative business practices to continue unabated.

This legislation, drafted by industry and passed with little debate, seeks to confuse the conversation and provide cover for deep-pocketed groups to change the conversation from one about strong protections for consumers to one about “harmonizing” protections. But these bills represent a race to the bottom, and are often deeply flawed. For instance, the Virginia bill includes problematic technical definitions of personal information, which exclude nearly all of the ad tech industry from its scope of opt-out. Under this law, it is not clear that the state will allow consumers to opt out of cross-contextual targeted advertising, the tracking of individuals across unaffiliated websites and services. Any law passed by Congress should build upon the work done by states that does protect their consumers, and not preempt state laws that seek to provide additional protections to those enacted by Congress.

Congress should give the Federal Trade Commission a legal mandate to enforce privacy laws beyond those bad actions that are deceptive or unfair. This is doubly true since—for certain historical reasons—the Commission rarely initiates privacy cases under its unfairness authority. The agency’s existing authority to regulate privacy, in practice, limits it to taking action only after a company has made an explicit promise to consumers and then broken that promise. This is well short of the robust protections necessary to ensure the privacy and security of consumers’ data.

Strong FTC enforcement authority, such as measures proposed by many members of this Committee, is essential, as are the provisions granting the state attorneys general and private consumers the authority to bring suit. Together, they would enable the Commission to undertake a robust enforcement regime, and empower consumers and state law enforcement to step in when the Commission cannot or will not do so.

Expanding FTC Capacity

The Agency Currently Has Few Privacy Staffers

Expanding the agency’s capacity to enforce the law is also critical. Laws alone without enforcement don’t protect the public. Presently, the Commission’s Division of Privacy and Identity Protection (DPIP) is tasked with solving the Nation’s myriad privacy and cybersecurity issues with a bare-bones staff of about 40 attorneys and a handful of technologists. In comparison, European countries have robust laws, such as the General Data Protection Regulation (GDPR). Each country typically has a Data Protection Agency (DPA) with hundreds of staff and dozens, if not hundreds of technologists. For example, the German DPA has 745 staff and nearly 100 tech experts enforcing their law for a country with one quarter the population of the

United States.¹ Similarly, France, which has one-fifth our population, employs nearly 200 staff, including 30 tech experts. The nations that employ the most technologists have had the most success in bringing corrective actions against big technology companies.²

The FTC, with its 40 staff and fewer than 10 technologists, simply does not have enough resources to police an industry that touches nearly every aspect of the American economy. This leads the agency to prioritize certain cases, and ignore privacy violations if they aren't deemed sufficiently harmful or easy to prosecute, or if the staff hours aren't available. If staff are already engaged in one privacy or security matter, they may simply ignore harmful acts that arise while they are occupied.

The problem is exacerbated when businesses choose to litigate a case rather than accept a settlement. By some accounts, these cases can occupy one-third to half of the Commission's entire privacy division on a single matter. Again, that's half of the entire Federal privacy staff working on one case for years, at the exclusion of other critical work. Businesses and their lawyers know and exploit this: in my experience, when outside counsel knows that the Commission has its hands full with litigation, they recommend that their clients take aggressive stances in response to FTC action, knowing that the FTC is unlikely to have the resources to adequately challenge them. Companies seek this expert knowledge, and hire former FTC officials to advise them on how to best avoid regulatory and enforcement scrutiny. Overworked commission staff have a hard time making up for this level of deliberate gamesmanship, and businesses' strategies to avoid FTC enforcement are quite successful.

The FTC Has Limited Enforcement Staff to Monitor Compliance

The FTC also does not have enough enforcement staff to monitor compliance with their orders. The Division of Enforcement—which is separate from DPIP, which investigates privacy violations—is tasked with overseeing compliance with *all* of the Commission's consent decrees, in addition to the myriad of laws relating to Made In USA and textile labeling, for example.³ The same lawyers who ensure that social media companies have robust privacy and data security programs are making sure labels on bed linens are correct. Technology enforcement requires its own nuanced set of skills, and the FTC needs both numbers and staff with special knowledge. Current enforcement staff have varying skill sets, and while they may be generalists, they may well not understand algorithms, APIs, or data encryption.

The Commission needs not only enough staff to monitor compliance with their orders, it needs that staff to have the expertise to understand the complex technological principles the initial violation was based on. Presently, the staff who investigate and bring a matter are not the ones who handle enforcement of consent decrees for those matters. The staff disconnect often results in a huge gap in expertise and understanding regarding what underlying privacy violations occurred. Ideally, the Commission should have enough staff to leverage the expertise of the initial investigators as part of the enforcement oversight process.

In fact, many of the “Big Tech” companies with which Congress is presently concerned—such as Facebook, Apple, Google, and others—are already under consent decree with the Commission. The companies have already taken some action that has landed them—essentially—under probation with the Commission, and have agreed to a set of negotiated terms with the agency. While this appears reasonable on paper, these orders don't do much to curb problematic practices: staff limitations at the agency mean that enforcement is lax or non-existent. For instance, one common enforcement tool is to require companies to submit regular third-party assessments of their data practices. These third-party assessments can provide the Commission insight into ongoing compliance by the company. But these assessments are only made available to the FTC upon request, and the Commission staff rarely has time to request them. In fact, one former FTC enforcement staff has publicly stated that the FTC rarely even reads these assessments.⁴

Under the current arrangements at the FTC, it is quite possible—even likely—that at least some of the companies under order are violating the terms of their

¹Irish Council for Civil Liberties, *Europe's Enforcement Paralysis* 10 (2021), <https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf>.

²*Id.* at 7 (noting that Germany has taken 16 and France 19 corrective actions versus two or three actions taken on average by every other member state).

³Federal Trade Commission, *What We Do*, <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>.

⁴Megan Gray, *Understanding and Improving Privacy 'Audits' Under FTC Orders* (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3165143.

agreement but that the Commission doesn't have the adequate resources to properly investigate.

The FTC Has Limited Technologists on Staff

In 2010, I was one of the first two technologists ever hired by the Federal Trade Commission to work on privacy matters in DPIP. My workload quickly went from handling small portions of matters to being deeply involved in nearly every case brought by the Commission. I personally helped to bring the Commission's first major successful cases against Twitter, Google, and Facebook. I have firsthand experience with how important technologists are to the effective oversight of big technology companies.⁵

Despite this, the Commission only has a limited number of technology experts on staff. When I re-joined the agency in 2014, as Chief Technology Officer, there was only one other technologist on staff. With the support of the then-Chair Ramirez, I helped to create the Office of Technology Research and Investigation (OTech) and grew that number of technologists to approximately ten by the end of my term in 2016. But due to political pressures, these technologists were housed not as a separate division that could serve the entire agency, but instead in an obscure business unit within the IT staff of the Bureau of Consumer Protection (BCP): the same group that maintains eDiscovery computers and other litigation support resources for the Commission. This awkward structure, which is in place to this day, effectively restricts the team by limiting their ability to report to key decision makers, and restricts them to functioning alongside the same group that provides IT support to investigators, dramatically reducing technologists influence across key investigations and policymaking.

Additionally, staff technologists frequently recuse themselves from active matters at the Commission due to the FTC's overly broad interpretation of rules prohibiting technologists from *ever* working on matters in which they participated during their employment at the Commission. Because of the unique nature of technologists' work, this same restriction does not apply to the attorneys or economists at the Commission, effectively penalizing technologists who work for the FTC. This overly broad provision intended to bar technologists from seeking post-FTC employment at many private companies on the same matters also prohibits them from working alongside the FTC in civil enforcement at state agencies, including, as was my experience, for the offices of state attorneys general.⁶

Even in its hobbled structure, OTech was able to help support the Commission's staff by providing trainings on emerging technology issues, giving briefings on topics as varied as "advertising industry market dynamics, online manipulation, creepware apps, misuse of payment data from web skimming, methods of detecting deepfakes and authenticating original media, and using mobile phone data to inform COVID-19 public health response," according to their budget justification for 2022.⁷ Expanding the role and influence of this group will greatly aid consumer protection efforts by the Commission on key topics of interest to Congress

Creating a New FTC Bureau

Incentivizing Collaboration and Efficiency at the FTC

Providing additional resources to the FTC is an essential first step to empowering the Commission to pursue strong technology enforcement. A new bureau, funded fully, will ensure that the Commission can fulfill its mission, and I support the measure. However, it is essential that the creation of a new bureau enables the Commission to collaborate and leverage its resources to investigate fully the wide range of harms caused by new technology and data practices.

To ensure that funding and additional resources are most effective, Congress should make clear that collaboration between all of the bureaus is an important goal of its funding. Too often, the bureaus at the FTC work in isolation, creating silos that fail to maximize the expertise throughout the Commission. For example, BCP houses the Division of Marketing Practices (which investigates fraud), the Division of Advertising Practices (investigating influencers and major advertising practices),

⁵ See also, Matt Burgess, *How France Tamed Google*, Wired (Aug. 2, 2021), <https://www.wired.co.uk/article/google-france-fines> (explaining that the success of the major French antitrust case against Google was due to the agency relying on technologists, rather than lawyers, to build the case).

⁶ Lindsey Barrett, Laura Moy, Paul Ohm & Ashkan Soltani, *Illusory Conflicts: Post-Employment Clearance Procedures and the FTC's Technological Expertise*, 35 Berkeley Tech. L. J. 793 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895823.

⁷ Federal Trade Commission, Congressional Budget Justification Fiscal Year 2022 at 63, <https://www.ftc.gov/system/files/documents/reports/fy-2022-congressional-budget-justification/fy22cbj.pdf>.

and the Division of Privacy and Identity Protection (investigating privacy and identity theft). These three divisions often look into the same entities for related matters, but do not often collaborate across the divisions.

Under this structure, cases that deal with financial practices issues in one division could miss the digital harms that pervade the business practices at issue. Fortunately, there appears to have been cross-division collaboration in a recent Financial Practices case: Venmo—likely due to technology staff who are better able to move between these boundaries. But in my experience, cross-division collaboration is unfortunately not the norm which creates inefficiencies and challenges when investigating fast-moving and well resourced industry players.

Technology and Data Protection: A New Bureau By Any Other Name

One way to incentivize collaboration and forward-looking enforcement is to appropriately scope any new bureau to reflect the underlying needs of the current digital ecosystem. Data security, data abuse, and identity theft all have one thing in common: technology and the underlying data they rely on. Narrowly constraining a new bureau on solely one of those practices, privacy, and giving it a name that reflects that narrow focus, would fall short of the consumer protection goals laid out for the FTC and by Congress. Instead, the bureau's mission and name should reflect the realities of current challenges: *The Bureau of Technology and Data Protection*.

This may seem like a small point, but names do matter. Many of the harms that concern this Committee and are investigated by the Commission do not fall neatly into the category of “privacy” harms. Instead, many are abuses of personal data, harms to civil rights or liberties, abuses of kids’ data that fall outside of COPPA, and the intentional design and release of harmful products.⁸ Data firms often innovate new ways to track or identify users without consent, and cannot easily be cabined by a singular focus on “privacy.”⁹ Other harms, such as algorithmic bias or hyper-targeted news feeds and recommendation algorithms, also do not fit neatly into “privacy” as a category. A new bureau should be empowered to investigate these data practices: their disproportionate effects on minorities and other vulnerable populations, are often what harm consumers the most, and often do not fall squarely into “privacy.”

I have long advocated for the creation of a new Bureau of Technology and Data Protection, because technology and *data* pervades nearly every case that comes before the Commission. Congress should create a bureau with the mission and expertise to investigate harmful practices across the technology ecosystem and support the existing divisions—like the Division of Privacy and Identity Protection, Ad Practices, and Marketing Practices—in order to better protect vulnerable populations. This Bureau of Technology and Data Protection could issue guidance to staff about how to approach technology in matters and could support investigations across the entire range of digital harms the commission addresses.

A Bureau of Technology and Data Protection would provide a “hub” of resources for the Commission that would serve across the agency’s many consumer protection missions, incentivize collaboration across agency divisions, and encourage efficiency. The Commission could look to the Bureau of Economics (BE) as a model. Similarly to BE, the new bureau should perform research and investigations to help support the Commission’s mission. The new bureau can also function as a community of practice and expertise within the Commission that informs other divisions and the FTC as a whole. When necessary, employees of the new bureau, including technologists and other experts, could be detailed to other bureaus or groups to support ongoing matters that may benefit from their expertise. These meaningful opportunities for collaboration and education will create a more robust culture within the FTC, and help draw talent.

The FTC needs more resources, but it also needs the right resources. Narrowly focusing the bureau’s expertise on “privacy,” rather than a broader mission of data practices generally, would create structural limitations that will live on in the Commission for years to come.

Recommendations

I’d like to briefly lay out a few concrete recommendations for this Committee to consider as it moves forward on privacy legislation, either in this current legislation or later.

⁸K.G. Orphanides, *Children’s YouTube Is Still Churning Out Blood, Suicide and Cannibalism*, Wired (Mar. 23, 2018), <https://www.wired.co.uk/article/youtube-for-kids-videos-problems-algorithm-recommend>.

⁹See, e.g., Geoffrey A. Hunter & Tatum Fowler, *When You ‘Ask App Not to Track,’ Some iPhone Apps Keep Snooping Anyway*, Wash. Post (Sept. 23, 2021), <https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/>.

First, this Committee should focus on the outcomes it seeks to enable, rather than becoming entangled in the details of agency organization. While additional resources and bureaus are important, it is important to implement change in ways that avoid bureaucratic siloing or creating divisions between staff at the agency that may well be counterproductive to ensuring a strong privacy enforcement regime. Instead, the Committee should focus on creating incentives and resources for the agency to hire experts and seek collaborative solutions to continuing market problems.

For instance, many of the most pressing harms this Committee is concerned with, such as the psychological harms caused to teens by social media,¹⁰ do not fit cleanly into existing privacy enforcement tools. The Committee should seek to enable the Commission to seek remedies for digital conduct that causes harm, even when the practice doesn't fall neatly under deceptive or unfair practices. Additional enforcement authorities, such as enabling the Commission to protect against negligent design or abusive business practices, would go a long way to protecting consumers in the digital age.

This Committee could address these harms by providing guidance to the Commission with the funding of this Bureau. For instance, by directing the Commission to conduct a rulemaking to reduce the instances of identity theft or ransomware attacks online, to increase safeguards around extractive data practices (such as micro-targeting), or to protect populations that are particularly vulnerable online, such as communities of color, the LGBTQ+ community, women, and children.

Similarly, the Committee could greatly reduce the burden on consumers by directing the FTC, as Senator Blumenthal already has,¹¹ to adopt a Global Privacy Control (GPC) as a legally adequate opt-out mechanism.

Alongside additional funding and Congressional direction, the Committee should take steps to ensure that the Commission hires a wide range of staff outside its traditional lawyers, economists, and technologists. In addition to those professionals, the agency should hire statisticians, designers, social scientists and behavioral researchers, such as experts on child development, who can guide complex cases that come before them. These experts would allow the FTC to review product documents at their earliest stages, understand complex project calculations, and identify manipulative designs. Additional expertise will also help the agency identify the current business practices and apps might contravene existing Section 5 authority and empower the agency to more fully use its existing enforcement tools.

Further, the Commission should devote more energy to developing and retaining its talent outside the traditional Washington, DC pool. It should take steps to hire talented individuals from across the country, not just Washington. The pandemic showed that remote work is possible, and in many circumstances desirable; hiring nationwide, to remote positions, and in the regional offices, would better enable the Commission to compete for talent with the firms it oversees.

Once the Commission has talent in the door, it needs to do a better job of retaining it. Technologists' pay should be raised to be more competitive with technology salaries, which are often many times higher than what the Commission offers. Technologists also need to be able to complete meaningful and engaging work at the Commission without worry that the FTC's obtuse conflicts rules will prevent them from seeking future employment later in their careers. Congress should seek answers from the FTC about how the Commission will clarify and update its conflict rules in order to better attract technologist talent.¹²

Conclusion

The creation of a new bureau at the Commission would be an important step forward, but it is not the only important change that is needed, and the work can't stop there. With a new bureau, the United States will gain a stronger Federal Data Protection enforcer, which will help allay concerns from Europe, and keep us competitive on a global scale.

The new bureau needs not just money, however, but additional substantive authority to investigate and curtail harmful data practices and to rely on Commission resources. These necessary tools include straightforward legislative fixes, such as providing the Commission with first-time civil penalty authority. As the Committee

¹⁰Georgia Wells, Jeff Horowitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, Wall St. J. (Sept. 14, 2021), <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739>.

¹¹Letter from Senator Blumenthal, Senator, to FTC Chair Lina Khan (Sept. 20, 2021), <https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf>.

¹²Lindsey Barrett, Laura Moy, Paul Ohm & Ashkan Soltani, *Illusory Conflicts: Post-Employment Clearance Procedures and the FTC's Technological Expertise*, 35 Berkeley Tech. L. J. 793, 826 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895823.

continues to pursue this matter, it should strongly prioritize drafting and passing a comprehensive data privacy law that empowers Federal regulators, including the FTC.

Congress should consider meaningful protections for consumers, including strengthening the Commission, ensuring the attraction and retention of talented Federal staff, and ensuring that there are robust laws on the books to protect American consumers.

ILLUSORY CONFLICTS: POST-EMPLOYMENT CLEARANCE PROCEDURES AND THE FTC'S TECHNOLOGICAL EXPERTISE

Lindsey Barrett[†], Laura Moy^{††}, Paul Ohm^{†††} & Ashkan Soltani[‡]

ABSTRACT

The Federal government restricts what former employees can work on after they leave the government, and for good reason. These post-employment conflict restrictions attempt to address the “revolving door” problem, where employees take information learned from their position in government to unfairly advantage industry. But an unintended consequence of overbroad conflict rules is that they impede well-meaning, former Federal employees from providing their knowledge and general expertise to other enforcement agencies with similar missions, such as those at the state level. This is playing out right now with FTC technologists, at a time when the agency—and, indeed, consumer protection agencies more broadly—desperately needs greater technical expertise. Three problems result: (1) former FTC technologists find themselves unable to contribute to the enforcement efforts of other agencies and plaintiffs’ attorneys aligned with the mission of the FTC, (2) some current FTC technologists are unwilling to work on important issues before the agency out of fear that doing so will limit their ability to work on related matters in the future, and (3) would-be technologists may be unwilling to take a position at the agency due to these concerns.

We explore the impact of Federal conflict rules on technologists working with the FTC, consider how this impact has changed alongside changing circumstances and enforcement practices, and discuss policy implications. We conclude that unless the FTC reforms the way it administers its conflict rules, it risks losing the assistance of technological expertise—expertise of which it badly needs more, rather than less.

TABLE OF CONTENTS

I. INTRODUCTION

II. FEDERAL POST-EMPLOYMENT RESTRICTIONS

A. HISTORY AND GOALS OF FEDERAL POST-EMPLOYMENT RESTRICTIONS

B. POST-EMPLOYMENT CONFLICT OF INTEREST RESTRICTIONS UNDER 18 U.S.C. § 207

C. POST-EMPLOYMENT CONFLICT OF INTEREST RESTRICTIONS UNDER FTC RULES

III. POST-EMPLOYMENT RESTRICTIONS IN FTC PRACTICE TODAY

A. IMPACT OF POST-EMPLOYMENT RESTRICTIONS ON TECHNOLOGISTS

B. INCREASED MARKET CONSOLIDATION

C. TECHNOLOGISTS ACT AS UTILITY PLAYERS

DOI: <https://doi.org/10.15779/Z38901ZG6Z>

© 2020 Lindsey Barrett, Laura Moy, Paul Ohm & Ashkan Soltani.

[†]Adjunct Professor of Law and Fritz Family Fellow, Georgetown University Law Center.

^{††}Associate Professor of Law and Director of the Communications & Technology Law Clinic, Georgetown University Law Center.

^{†††}Professor of Law and Associate Dean, Georgetown University Law Center. From 2012–13, Professor Ohm served as a Senior Policy Advisor for Privacy in the FTC’s Office of Policy Planning.

[‡]Distinguished Fellow, Institute for Technology Law & Policy and Center on Privacy & Technology at Georgetown University Law Center. From 2010–11, Mr. Soltani served as a staff technologist for the Division of Privacy and Identity Protection at the FTC. And from 2014–16, Mr. Soltani was appointed as the Chief Technologist of the FTC, wherein he helped in creating the Office of Technology Research and Investigation in order to expand the FTC’s roster of technologists. The authors are grateful to Harsimar Dhanoa and Jeffrey Brown for excellent research assistance. They are also grateful to Chris Hoofnagle, Jessica Rich, and David Vladeck for helpful comments.

D. LENGTHY AND BROAD CONSENT DECREES

E. RISK-AVERSE AGENCY CULTURE

F. POSSIBLE POLITICAL CONFLICT BETWEEN FTC AND STATE ATTORNEYS GENERAL

IV. IMPLICATIONS FOR AGENCY EFFICACY

V. POLICY RECOMMENDATIONS

VI. CONCLUSION

I. INTRODUCTION

The Federal Trade Commission's (FTC) laudable decade-long experiment to hire in-house technologists may be in jeopardy from an unexpectedly bureaucratic source: Federal conflict of interest law. Post-employment restrictions for Federal employees are designed to ensure that government officials avoid corruption and to slow the revolving door into industry. In their current application to former technologists, however, they have the counterproductive effect of preventing people with technical expertise from engaging in work that creates no meaningful conflicts.

Preventing technologists from accepting unproblematic post-government work through the conflicts clearance process harms the consumer protection and pro-competition missions of the agency. Overbroad conflicts clearance policies harm the direct mission of the agency by limiting the ability of experts to aid fellow enforcers such as state attorneys general, who should be seen as force multipliers or fellow travelers in policing technology companies. These policies also make it more difficult for the FTC to hire and retain technological experts, which hampers the agency's ability to adequately fulfill its competition and consumer protection missions. Prospective technologists think twice about working for the agency when they hear about the way the clearance process has limited the activity of others. FTC employees also limit the cases they can work on in order to avoid potential post-employment conflicts.

This paper builds on the direct experience of two of the authors, one a former Chief Technologist and the other a former Senior Policy Advisor for privacy at the FTC. Since leaving the agency, we have encountered numerous obstacles in our experience with the FTC's clearance process, which we find to be unnecessarily broad in design and perhaps also in execution. We have bolstered this firsthand experience through interviews with numerous former FTC officials who confirm and expand upon our observations.

We begin with an outline of our methodology. We interviewed eight former FTC consumer protection attorneys and technologists and two attorneys in the offices of state attorneys general in order to assess the extent of the problem. The goal of the interviews was to determine whether the experience of two of us being denied the ability to work on certain matters post-FTC employment was representative, whether technologists and other specialists were treated differently for the purpose of conflicts, and whether there was any consensus as to why the FTC was applying the conflicts rules the way it was and still is.

Preserving anonymity to allow our interviewees to discuss sensitive topics was and is a key concern, given how few former technologists there are and how easily certain details would reveal the identity of the interviewees. For the reader's edification, we have tried to provide as much context as possible without compromising the anonymity of the interviewees, such as by highlighting when statements were contradicted by other interviewees, not contradicted by any interviewees, supported by interviewees, supported by only some interviewees, or when they were supported indirectly. Indeed, the difficulty of preserving the anonymity of our interviewees underscores the very problem enumerated in this essay—there are simply too few FTC technologists for the answers we describe here to allow each subject to get lost in a crowd.

We focus on the FTC because that is the agency with which we have direct experience, but the lessons of our analysis may also apply to other government agencies seeking to hire and retain technological experts, which ought to describe nearly every agency in this technological age. The way an agency interprets the conflict of interest laws and the way it administers its clearance procedures can have an important, underappreciated impact on the way it fulfills its mission—and the ability of other enforcers to fulfill theirs.

Part II of this Article explains why the Federal conflict rules were created and how they affected current and former agency employees at that time. Part III discusses how changes in technology, economy, market, and agency practices have altered the impact of these conflict rules on technologists working with the FTC. Part IV explores the implications of this changing impact on agency efficacy and on the

FTC's ability to handle technical and other specialized subject matters. Part V offers policy recommendations to address this problem to help pave the way for the FTC and other Federal agencies to increase their technical capacity, in part by hiring technical specialists.

II. FEDERAL POST-EMPLOYMENT RESTRICTIONS

Federal law restricts post-government employment opportunities for all Federal government employees. The primary source of these restrictions across the Federal government comes from one Federal ethics statute, 18 U.S.C. § 207. In addition to § 207, former FTC employees must comply with post-employment restrictions set forth in the FTC Rules of Practice (*i.e.*, 16 C.F.R. § 4.1(b)). As a starting point, it is helpful to understand more about the history, origin, and intent of these restrictions, as well as what they do and who interprets and enforces them.

A. HISTORY AND GOALS OF FEDERAL POST-EMPLOYMENT RESTRICTIONS

Both the Federal conflict statute and the FTC's conflict rules were established in the 1960s.¹ Legislative and administrative history show that restrictions on where a former Federal employee may work and what matters they may work on are intended to combat the "revolving door" problem and to prevent both actual government corruption and the appearance thereof.² The rules are nevertheless intended to be somewhat restrained, balancing the need to combat these problems with the need to preserve the government's ability to attract and retain top-notch expertise.³ Striking the right balance between these competing objectives—preventing corruption and facilitating expertise—is key to optimizing government function.

The Federal statute designed to prevent actual and perceived conflict by former Federal employees, § 207, was developed on the belief "that a public servant owes undivided loyalty to the Government."⁴ The statute addresses two primary ways in which potential conflicts might occur. First, former Federal employees could "switch sides" upon leaving the government, going on to provide other parties with an agency's proprietary information in an adversarial proceeding, which would limit the agency's ability to protect the public interest.⁵ Second, if Federal employees anticipate using their Federal experience to help secure lucrative post-agency employment at a regulated entity, they might temper their behavior while employed by the agency.⁶ Lax rules for post-agency employment conflicts would invite Federal employees to mold their conduct at the agency to make themselves more appealing candidates for employment at a regulated entity after leaving the agency. The legislative history and subsequent cases interpreting the statute and rules also reflect a concern

¹ 18 U.S.C. § 207 was established in 1962 alongside several other Federal anti-corruption provisions. Act to Strengthen the Criminal Laws Relating to Bribery, Graft, and Conflicts of Interest, and for Other Purposes, ch. 11, §§ 201–09, 218, 76 Stat. 1119–25 (1962). 116 C.F.R. § 4.1(b) was established in 1967. Commercial Practices, 32 Fed. Reg. 8444, 8456–59 (June 13, 1967).

² See S. REP. NO. 95–170, at 32 (1977) ("18 USC 207, like other conflict of interest statutes, seeks to avoid even the appearance of public office being used for personal or private gain. In striving for public confidence in the integrity of government, it is imperative to remember that what appears to be true is often as important as what is true. Thus government in its dealings must make every reasonable effort to avoid even the appearance of conflict of interest and favoritism." (emphasis in original)).

³ See *id.* ("But, as with other desirable policies, it can be pressed too far. Conflict of interest standards must be balanced with the government's objective in attracting experienced and qualified persons to public service. Both are important, and a conflicts policy cannot focus on one to the detriment of the other. There can be no doubt that overly stringent restrictions have a decidedly adverse impact on the government's ability to attract and retain able and experienced persons in Federal office.").

⁴ H.R. REP. NO. 87–145, at 3 (1961).

⁵ *Id.* at 4 ("[A]n official should be prohibited from resigning his position and 'switching sides' in a matter which was before him in his official capacity."); see also *United States v. Nasser*, 476 F.2d 1111, 1116 (7th Cir. 1973) (describing § 207 restrictions as serving to protect the government from use of agency information against the government); JACK MASKELL, CONG. RESEARCH SERV., POST-EMPLOYMENT, "REVOLVING DOOR," LAWS FOR FEDERAL PERSONNEL 1–2 (2014), <https://fas.org/sgp/crs/misc/R42728.pdf> ("One of the initial and earliest purposes of enacting the 'revolving door' laws was to protect the government against the use of proprietary information by former employees who might use that information on behalf of a private party in an adversarial type of proceeding or matter against the government, to the potential detriment of the public interest.").

⁶ MASKELL, *supra* note 5, at 2 ("Another interest of the government in revolving door restrictions was to limit the potential influence and allure that a lucrative private arrangement, or the prospect of such an arrangement, may have on a current Federal official when dealing with prospective private clients or future employers while still with the government, that is, 'that the government employee not be influenced in the performance of public duties by the thought of later reaping a benefit from a private individual.'") (quoting *Brown v. D.C. Bd. of Zoning Adjustment*, 413 A.2d 1276, 1282 (D.C. App. 1980)).

about the appearance of conflict, in addition to actual conflicts, because even the perception of corruption can erode public faith in the rule of law.⁷

Federal post-employment restrictions also aim to avoid being overly rigid. Overly rigid conflict rules might make it impossible to draw top talent to agencies where employees with needed expertise could easily find employment with other agencies or the private sector.⁸ Indeed, in enacting and revising § 207, Congress was acutely aware that restrictive rules could hamstring the government's ability to attract and retain technical experts. For example, in a 1960 House hearing on Federal conflict of interest legislation, a representative of the Department of Defense expressed concern that the proposed § 207 "would greatly narrow the opportunity for [people who came to government from private industry] to seek employment outside the Government if they were precluded thereafter from rendering any assistance to anyone in connection with any subject matter concerning which they had any responsibility."⁹ The Defense Department representative also pointed out that "[w]e have had considerable difficulty in recruiting engineers and scientists."¹⁰

As Congress deliberated over the structure and wording of conflicts restrictions in the year before passage of the bill that established § 207, President Kennedy sent a letter to Congress urging accommodations for temporary, part-time, and technical experts:

The fundamental defect of [conflict] statutes as presently written is that: On the one hand, they permit an astonishing range of private interests and activities by public officials which are wholly incompatible with the duties of public office; on the other hand, they create wholly unnecessary obstacles to recruiting qualified people for government service. This latter deficiency is particularly serious in the case of consultants and other temporary employees, and has been repeatedly recognized by Congress in its enactment of special exemption statutes. . . .

But if the statutes often leave important areas unregulated, they also often serve as a bar to securing important personal services for the government through excessive regulation when no ethical problem really exists. Fundamentally, this is because the statutes fail to take into account the role in our government of the part-time or intermittent adviser whose counsel has become essential but who cannot afford to be deprived of private benefits, or reasonably requested to deprive themselves, in the way now required by these laws. Wherever the government seeks the assistance of a highly skilled technician, be he scientist, accountant, lawyer, or economist, such problems are encountered.¹¹

The following decade, after the Watergate scandal, Congress passed the Ethics in Government Act, which revised and crafted new post-employment restrictions as part of a wave of reforms.¹² Before the new restrictions went into effect, however, a number of parties raised concerns that the restrictions might interfere with the hiring of high-caliber employees.¹³ In a report on the legislation, the Subcommittee

⁷ *Id.*; see also Adam Samaha, *Regulation for the Sake of Appearance*, 125 HARV. L. REV. 1563, 1599 (2011) (discussing ethics rules designed to facilitate public trust by diminishing the possible appearance of corruption).

⁸ MASKELL, *supra* note 5, at 2 ("These purposes in adopting limitations on former employees' private employment opportunities must, however, also be balanced against the deterrent effect that overly restrictive provisions on career movement and advancement will have upon recruiting qualified and competent persons to government service."); S. REP. NO. 95-170, at 32 (1977).

⁹ *Federal Conflict of Interest Legislation: Hearing on H.R. 1900, H.R. 2156, H.R. 2157, H.R. 6556, and H.R. 10575 Before the H.R. Antitrust Subcomm. of the Comm. on the Judiciary*, 86th Cong. 144 (1960) (statement of Stephen S. Jackson, Deputy Assistant Secretary of Defense for Manpower, Personnel, and Reserve).

¹⁰ *Id.*

¹¹ President's Special Message to the Congress on Conflict-of-Interest Legislation and on Problems of Ethics in Government, 1961 PUB. PAPERS 327-329 (Apr. 27, 1961).

¹² SAM BERGER & ALEX TAUSANOVITCH, CTR. FOR AM. PROGRESS, LESSONS FROM WATERGATE: PREPARING FOR POST-TRUMP REFORMS 3-6 (2018), <https://cdn.americanprogress.org/content/uploads/2018/07/27101947/WatergateReformsReport-3.pdf> (discussing the Ethics in Government Act and other "extensive" post-Watergate government reforms). Among other things, the 1978 Ethics in Government Act established "a mechanism for the appointment of an independent special prosecutor"; created the Office of Government Ethics; and "imposed the first mandatory financial disclosures for members of Congress, candidates, and some high-level Executive Branch officials." *Id.*

¹³ STAFF OF THE SUBCOMM. ON OVERSIGHT & INVESTIGATIONS OF THE H. COMM. ON INTERSTATE & FOREIGN COMMERCE, 96TH CONG., CONG. REP. ON IMPACT OF THE ETHICS IN GOV'T ACT 5 (Comm. Print 1979).

on Oversight and Investigations of the House Committee on Interstate and Foreign Commerce explained that ethics restrictions should “accommodate the need to attract and retain a qualified and experienced work force.”¹⁴ The report also stated that “hearings reflected the grave concern of agency heads” that the “balance between maintaining integrity and ensuring an able workforce has not been properly struck.”¹⁵ For example, the Secretary of Health, Education, and Welfare characterized the revisions as likely to cause “the greatest brain drain of talent in the history of Federal service.”¹⁶ Recognizing the need to strike a balance between preventing conflicts and attracting top talent, Congress ultimately softened the new limitations before they went into effect.¹⁷

B. POST-EMPLOYMENT CONFLICT OF INTEREST RESTRICTIONS UNDER 18 U.S.C. § 207

The Federal statute defining post-employment conflicts, § 207, is both a criminal and a civil statute; those who violate it could end up in prison or be subject to a hefty civil penalty.¹⁸ The statute is enforced by the Department of Justice (DOJ),¹⁹ but the Office of Government Ethics (OGE) has regulatory authority to promulgate rules, providing further details on the application of § 207 beyond what is provided in the statute.²⁰ In addition, the FTC provides direct guidance to former employees regarding § 207.²¹ Under § 207, former Federal employees are not prohibited from taking a job with any other potential employer but are prohibited from engaging in certain activities.²² For former FTC employees, there are two types of conduct prohibited under the Federal statute of which they should be aware.

First, the Federal statute essentially prohibits a former Federal employee from switching sides on a matter on which they previously represented the Federal government.²³ If a former FTC employee communicates to, or appears before, the Federal government as a part of their new job with the intent to influence “in connection with a particular matter . . . in which the person participated personally and substantially” as a Federal employee, that behavior constitutes a violation.²⁴ This prohibition lasts forever.

Second, even for a matter in which the former Federal employee did *not* “participate[] personally and substantially,” § 207 still prohibits the person from working on it if the person “knows or reasonably should know [the matter] was actually pending under his or her official responsibility . . . within a period of 1 year before the termination” of their employment.²⁵ This restriction expires after two years.²⁶

In determining whether a former matter and a post-employment matter are the same, OGE rules state that “all relevant factors should be considered, including the

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ OFFICE OF GOV'T ETHICS, REPORT TO THE PRESIDENT AND TO CONGRESSIONAL COMMITTEES ON THE CONFLICT OF INTEREST LAWS RELATING TO EXECUTIVE BRANCH EMPLOYMENT 14 (2006) (“Before these new restrictions even became effective, Congress amended section 207 to lighten the new restrictions, in response to expressions of concern about the expected impact on recruitment and retention.”).

¹⁸ An offense can result in up to a year in prison, and a willful offense can result in up to five years. 18 U.S.C. § 216(a) (2018). In addition, a person who violates § 207 can be subject to a civil penalty up to fifty-thousand dollars for each violation or the amount of compensation which they received for the prohibited conduct, whichever amount is greater. 18 U.S.C. § 216(b).

¹⁹ Post-Employment Conflict of Interest Restrictions, 5 C.F.R. § 2641.103(a) (2020).

²⁰ 5 C.F.R. § 2638.108(a)(1).

²¹ See 5 C.F.R. § 2641.105(a) (stating that “[t]he agency in which an individual formerly served has the primary responsibility to provide oral or written advice concerning a former employee’s post-employment activities,” including regarding § 207). This is consistent with our experience. Staff of the FTC’s Office of General Counsel have provided us with guidance and advice regarding the application of § 207 to post-employment activities that we have inquired about.

²² 18 U.S.C. § 207; see Office of Gov’t Ethics, *supra* note 17, at 11 (“None of its provisions bars any individual, regardless of rank or position, from accepting employment with any private or public employer after Government service. Section 207 only prohibits former employees from engaging in certain activities on behalf of persons or entities other than the United States, whether or not done for compensation.”).

²³ 18 U.S.C. § 207; see MASKELL, *supra* note 5, at 2–3; United States v. Nasser, 476 F.2d 1111, 1116 (7th Cir. 1973) (holding in favor of constitutionality of prohibition language).

²⁴ 18 U.S.C. § 207(a)(1). This only applies when the matter also is one “in which the United States or the District of Columbia is a party or has a direct and substantial interest,” and “which involved a specific party or specific parties at the time” the former employee worked on it. *Id.* Former Federal employees also cannot engage in this variety of prohibited communications and/or appearances before the District of Columbia. *Id.*

²⁵ 18 U.S.C. § 207(a)(1)–(2).

²⁶ *Id.* For a more fulsome explanation of the provisions of § 207, including restrictions not discussed here, see MASKELL, *supra* note 5, at 3–6.

extent to which the matters involve the same basic facts, the same or related parties, related issues, the same confidential information, and the amount of time elapsed.”²⁷

§ 207(j) lays out a number of exceptions to these general restrictions. For example, under this subsection, former employees are exempted from certain post-employment restrictions to carry out official duties as a Federal employee, state or local government official, or representative of a higher education institution. One exception that is particularly relevant to agency technologists is an exception under several provisions of § 207 for “communications [made] solely for the purpose of furnishing scientific or technological information, if such communications are made under procedures acceptable to the department or agency concerned.”²⁸

As noted above, § 207 is enforced by the DOJ.²⁹ Accordingly, an agency where a former Federal employee served—such as the FTC—does not have the authority to determine definitively how § 207 applies to a former employee, but the agency is responsible for providing former employees with advice regarding the application of § 207 to post-employment activities.³⁰ In determining whether and how to pursue prosecution under § 207, however, the DOJ may take into account a former Federal employee’s reliance on advice received from the agency where they formerly served.³¹

C. POST-EMPLOYMENT CONFLICT OF INTEREST RESTRICTIONS UNDER FTC RULES

The FTC’s rules also restrict what matters a former employee can work on after their employment with the FTC ends.³² Generally speaking, the FTC’s post-employment conflict rules prohibit former employees from communicating to or appearing before the FTC and from assisting or advising behind-the-scenes regarding certain “proceeding[s] or investigation[s].”³³

Most relevant to former technologists is § 4.1(b) of the FTC’s rules.³⁴ After leaving the agency, a former employee generally cannot work on a proceeding or investigation that is the same as one in which they “participated” on behalf of the agency.³⁵ A former employee also cannot later work on a proceeding or investigation if they received or saw “nonpublic documents or information” pertaining to it while working for the agency.³⁶ These restrictions are permanent, but the FTC’s rules also establish certain time-limited restrictions for former employees.³⁷

There is no bright-line rule that enables a former employee to conclude with certainty that an activity in which they would like to engage constitutes the same “proceeding or investigation” as one in which they participated while employed by the FTC. According to a note in the FTC’s rules, “a new ‘proceeding or investigation’ may be considered the same matter as a seemingly separate ‘proceeding or investigation’ that was pending during the former employee’s tenure.”³⁸ In assessing this differentiation, “the Commission . . . consider[s]: the extent to which the matters involve the same or related facts, issues, confidential information and parties; the time elapsed; and the continuing existence of an important Federal interest.”³⁹ These criteria are nearly identical to the criteria considered by the OGE in determining whether a former matter and post-employment matter are the same under § 207.⁴⁰

The FTC’s rules also set forth a formal process to help former employees determine whether or not they are indeed restricted from working on a matter in their non-FTC employment capacity.⁴¹ In certain circumstances, a former employee is re-

²⁷ 5 C.F.R. § 2641.201(h)(5)(i).

²⁸ 18 U.S.C. § 207(j)(5).

²⁹ 5 C.F.R. § 2641.103(a).

³⁰ 5 C.F.R. § 2641.105(a).

³¹ 5 C.F.R. § 2641.105(c).

³² 16 C.F.R. § 4.1(b)(1) (2020).

³³ *Id.*; see *Post-Employment Restrictions*, FED. TRADE COMM’N, <https://www.ftc.gov/about-ftc/bureaus-offices/office-general-counsel/post-employment-restrictions> (last visited Aug. 22, 2020).

³⁴ 16 C.F.R. § 4.1(b).

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.* A former employee cannot work on a proceeding or investigation that was pending under their official responsibility within a year of when they left the agency. *Id.* This restriction lasts for two years after an employee leaves the agency. *Id.* In addition, for one year after leaving the agency, Commissioners and “senior employees” cannot work on any proceeding or investigation before the FTC. *Id.*

³⁸ 16 C.F.R. § 4.1(b)(1) n.1.

³⁹ *Id.*

⁴⁰ See 5 C.F.R. § 2641.201(h)(5)(i).

⁴¹ See 16 C.F.R. § 4.1(b)(2).

quired to file a “request for clearance” to participate in a matter that is or was before the FTC.⁴² If the former employee left the agency within the previous three years, these circumstances include when the proceeding or investigation was pending before the FTC while the former employee was there, when the matter is the direct result of another proceeding or investigation that was pending before the FTC while the former employee was there, or when “nonpublic documents or information” pertaining to the matter were seen (or likely would have been seen) by the former employee as part of their work for the FTC.⁴³

After a former employee files a clearance request, the FTC’s Office of the General Counsel (OGC), or designee, has ten business days to respond by (1) granting the request, (2) stating that it recommends the FTC deny the request, or (3) extending its consideration of the request by up to ten additional business days.⁴⁴ If a former employee is not sure whether or not they need to file a clearance request, they can ask the General Counsel for advice.⁴⁵ The General Counsel or their designee will provide advice within three business days.⁴⁶

Significantly, the FTC’s rules grant the agency the discretion to simply decline to apply the rules to any specific set of circumstances. In addition, the rules do not apply to post-employment activities that would be covered if “otherwise specifically authorized by the Commission.”⁴⁷

While § 207 is enforced by the DOJ, the FTC’s post-employment conflict of interest restrictions are applied and enforced only by the FTC itself. To help current and former employees better understand the rules, the FTC provides guidance on its website.⁴⁸ The agency also gives new employees an ethics guide. The guide states: “if an FTC matter was open during your [*i.e.*, former employee’s] time here, you likely need to receive clearance before you work on it for a new employer. If you worked on the matter while at the FTC or had access to significant non-public FTC information about the matter, you are unlikely to get clearance.”⁴⁹

III. POST-EMPLOYMENT RESTRICTIONS IN FTC PRACTICE TODAY

As discussed above, post-government employment restrictions seek to balance the need to combat the revolving door and corruption with the need to preserve the government’s ability to attract and retain top-notch expertise. In the modern era, however, there is a greater need than ever in government—and perhaps especially in the FTC—for highly-skilled, technical expertise.⁵⁰ As a result, these restrictions appear to be off-balance with the FTC interpreting and applying post-government restrictions aggressively to combat the revolving door and corruption at the cost of attracting and retaining technical expertise. This is particularly true as applied to conduct that supports the FTC’s objectives and doesn’t implicate the corruption concerns that § 207 was designed to address. A former FTC technologist seeking to consult on a state attorney general investigation regarding consumer protection matters is better described as entering an adjoining wing than availing herself of a revolving door. Section III.A begins by identifying how post-employment restrictions arguably are failing to facilitate hiring and retention of skilled experts, specifically technologists. Why would the FTC administer conflict rules more broadly than necessary to advance the policy goals of preventing corruption and slowing the revolving door? Sections III.B–F identify several possible explanations, including increased market consolidation, the growing role of technologists as utility players, the length and breadth of consent decrees, the agency’s risk-averse culture, and possible political conflicts between the FTC and other enforcement agencies.

A. IMPACT OF POST-EMPLOYMENT RESTRICTIONS ON TECHNOLOGISTS

The FTC’s application of post-employment restrictions today goes beyond the policy goal of limiting corruption and the appearance of corruption.⁵¹ The FTC may also apply post-government employment restrictions too broadly in cases involving

⁴² *Id.*

⁴³ *Id.*

⁴⁴ 16 C.F.R. § 4.1(b)(7).

⁴⁵ 16 C.F.R. § 4.1(b)(6).

⁴⁶ *Id.*

⁴⁷ 16 C.F.R. § 4.1(b)(1).

⁴⁸ *Post-Employment Restrictions*, *supra* note 33.

⁴⁹ FED. TRADE COMM’N, LET’S TALK ETHICS: ETHICS ORIENTATION FOR NEW EMPLOYEES 7 (2019), https://www.ftc.gov/system/files/attachments/office-general-counsel/ieo_for_new_ftc_employees.pdf.

⁵⁰ For a discussion by the former FTC Commissioner on enforcement and oversight challenges created by rapidly changing technology and the possibility that the FTC is failing to keep up, see generally Terrell McSweeney, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. L. REV. 514 (2018).

⁵¹ See MASKELL, *supra* note 5, at 2.

former employees who want to work for the companies the FTC investigates, but we focus here primarily on circumstances for which there are clear public policy reasons to support a more permissive interpretation of post-employment restrictions: requests to work for state attorneys general seeking to investigate violations of law. In these cases, prohibiting former technologists from contributing does not serve the Federal conflicts provisions' goal of preventing employees from leaving the government and "switching sides." On the contrary, these other entities are best characterized as being on the *same side* as the FTC, and their law enforcement work is consonant with the consumer protection and pro-competition missions of the FTC.

As technologists and former FTC officials, two of us have encountered firsthand the FTC's broad interpretation of post-employment restrictions precluding us from contributing to valuable enforcement work by other agencies and plaintiffs. In addition, we conducted informal interviews of several other former FTC employees and technologists in order to ascertain additional information and context about how post-employment restrictions affect technologists.⁵²

From these interviews, we heard consistent variations on a theme: *there was general consensus that the rules were overly broad, their application opaque, and their impact felt acutely and disproportionately by former technologists*. While not everyone we spoke to had sought clearances themselves, many were aware of the process from colleagues. Several, however, had firsthand experience contacting the FTC to seek advice and, ultimately, clearance regarding matters they would like to work on that could be construed as related to matters they had worked on while employed by the FTC.

In particular, former technologists—ourselves included—have often been denied clearance by the FTC, under its own rules, to help others investigate entities subject to FTC enforcement even after a substantial period of time has passed. The crux of the problem is that the FTC often considers a state attorney general's current investigation regarding a major company to be the same "proceeding or investigation" as one conducted by the FTC of the same company for related practices—even if the FTC's investigation culminated in a complaint that has already been settled with the company in question.⁵³ The FTC further appears to consider technologists to have "participated personally and substantially" in its investigations of technology companies.⁵⁴

In other words, the FTC interprets its conflict rules as prohibiting us from working on the "same side" as the FTC in investigations that run parallel to the agency's mission. On at least three occasions, we have sought clearance to provide technical guidance to state attorneys general investigating the practices of major technology companies. Two of these requests for clearance were denied and the third took weeks to process. In fact, on one occasion, FTC staff told one of us directly that, even though providing assistance to a state attorney general would be working on the "same side" as the FTC, this was "irrelevant to the analysis" under FTC rules.⁵⁵

The conflicts rules are intended to prevent the appearance or actual existence of conflicts between current employees and companies the FTC oversees, not other enforcement entities.⁵⁶ By making it unduly difficult for former technologists to receive clearances, the agency makes it less attractive for technologists to work there and discourages those who do from working on certain cases, thus limiting the agency's own efficacy. This problem is intensifying as technological advancements in-

⁵² For a discussion of methodology, see *supra* Part I.

⁵³ 16 C.F.R. § 4.1(b)(1)(i) (restricting post-employment activities if "[t]he former employee participated personally and substantially on behalf of the Commission in the same proceeding or investigation in which the employee now intends to participate"). As discussed below, this problem likely is compounded by the fact that FTC consent decrees typically last for twenty years. *Infra* Section III.D.

⁵⁴ 16 C.F.R. § 4.1(b)(1)(i). As discussed below, this problem likely is compounded by the fact that FTC technologists are relied upon as utility players. *Infra* Section III.C.

⁵⁵ E-mail from Alternate Designated Agency Ethics Official, Office of the General Counsel, Federal Trade Commission, to one of the authors (Mar. 01, 2019, 08:00 EST) (on file with authors).

⁵⁶ See MASKELL, *supra* note 5, at 2 (identifying the animating goals of "revolving door" laws as "protect[ing] the government against the use of proprietary information by former employees who might use that information *on behalf of a private party* in an adversarial type of proceeding or matter against the government, to the potential detriment of the public interest," "limit[ing] the potential influence and allure that a lucrative *private* arrangement, or the prospect of such an arrangement, may have on a current Federal official when dealing with prospective *private* clients or future employers while still with the government," and "prevent[ing] the corrupting influence on the governmental processes of both legislating and administering the law that may occur, and the appearances of such influences, when a Federal official leaves his government post to 'cash in' on his 'inside' knowledge and personal influence with those persons remaining in the government.") (emphasis added).

crease the FTC's need for technical expertise.⁵⁷ In turn, this problem also makes other avenues in the U.S. enforcement ecosystem less effective because it limits the access of state attorneys general to qualified technology experts.

In addition to interpreting its own rules in this manner, the FTC also appears to interpret § 207 quite broadly. FTC staff have advised us that activities we sought to assist alongside state attorneys general could implicate § 207 as constituting the same matter as one in which we had participated at the FTC.⁵⁸

The FTC's procedural approach to former employees' conflict clearance inquiries raises additional problems. Based on our experience and that of the people we interviewed, it seems the FTC's OGC routinely denies clearance requests through an informal process completed over e-mail. The OGC sometimes advises former employees to submit a formal clearance request using a form designed for that purpose, but often does not. This approach limits the transparency of the decision, avenues for appeal, and rigor of the analysis.

B. INCREASED MARKET CONSOLIDATION

Increased market concentration and horizontal expansion in the technology sector also contribute to the agency's broad application of conflicts rules to technologists. In a diversified market, it can be easy to tell that a former FTC employee's work investigating Company A is not the same "matter" as, or is an unrelated "proceeding or investigation" to, work involving Company B. But when Company A is at the heart of both the prior investigation and the prospective work—perhaps because Company A acquired "nascent or potential competitor" Company B to eliminate a threat to Company A's market—the potential for conflict of interest may be higher.⁵⁹

There is no question that recent years have seen massive corporate consolidation, both vertical and horizontal.⁶⁰ The technology sector, in particular, exhibits a steady trend toward greater consolidation.⁶¹ For example, according to a recent report from the Open Markets Institute, the three largest social networking sites controlled eighty-five percent of the market in 2018, up from seventy-five percent in 2012; the two largest search engines controlled ninety-seven percent of the market in 2017, up from eighty-two percent in 2011; and the two largest e-commerce firms controlled fifty-six percent of the market in 2018, up from forty-six percent in 2016.⁶²

In addition to greater consolidation in the technology sector, the resultant diminished number of targets for enforcers to go after overall has provided all enforcement agencies—including the FTC—clear reasons to investigate the largest companies for violations of trade practice law. Precisely because of their outsized market shares, large companies that violate the law have the potential to cause substantial injury to large numbers of consumers.⁶³ And an enforcement agency with limited resources will get the greatest "bang for its buck" going after companies with large

⁵⁷ See generally McSweeney, *supra* note 50.

⁵⁸ 18 U.S.C. § 207(a)(1)(A) (restricting post-employment activities related to a particular matter "in which the United States or the District of Columbia is a party or has a direct and substantial interest").

⁵⁹ Press Release, Fed. Trade Comm'n, FTC to Examine Past Acquisitions by Large Technology Companies (Feb. 11, 2020), <https://www.ftc.gov/news-events/press-releases/2020/02/ftc-examine-past-acquisitions-large-technology-companies> (describing current FTC investigation of anti-competitive acquisitions by technology companies).

⁶⁰ *America's Concentration Crisis: An Open Markets Institute Report*, OPEN MKTS. INST., <https://concentrationcrisis.openmarketsinstitute.org/> (last visited Aug. 22, 2020) (illustrating the wave of consolidation across a wide range of industries over the past fifty years); Lina M. Kahn, *The Ideological Roots of America's Market Power Problem*, 127 YALE L.J.F. 960, 964 (2018), <http://www.yalelawjournal.org/forum/the-ideological-roots-of-americas-market-power-problem> (tracing the rise of concentration and the "cripple[ing]" of antitrust enforcement); David Leonhardt, *The Monopolization of America*, N.Y. TIMES (Nov. 25, 2018), <https://www.nytimes.com/2018/11/25/opinion/monopolies-in-the-us.html> (describing and opining on the Open Markets dataset).

⁶¹ Lina M. Kahn, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 710 (2017) (criticizing consumer welfare as ill-adapted to measure anti-competitive harms in the twenty-first century economy, particularly online platforms); Frank Pasquale, *When Antitrust Becomes Pro-Trust: The Digital Deformation of U.S. Competition Policy*, 2017 CPI ANTITRUST CHRON., May 2017, at 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3020163 (analyzing the consolidation of the technology sector and describing the failures of antitrust doctrine, and the interpretation and application thereof by U.S. regulators, to new trends).

⁶² *America's Concentration Crisis*, *supra* note 60. Although the specific search engines controlling the largest market share have changed between 2011 and 2017, the increase in the market share owned by the two largest companies at that time nevertheless reflects market consolidation.

⁶³ When it violates the law, a company that has a billion users has the potential to do greater harm than a company that has only a few thousand users.

numbers of users, substantial economic clout, and a high public profile, rather than going after smaller companies. Thus when the FTC announced its record five-billion-dollar settlement with Facebook in 2019, the size of the company was relevant: as the agency stated in its press release, “[m]ore than 185 million people in the United States and Canada use Facebook on a daily basis.”⁶⁴

A review of recent enforcement actions reveals that the enforcement efforts of the FTC and state attorneys general are indeed converging on a handful of companies. For example, in the last two years alone, Facebook has been both a target of the FTC and the subject of public investigations by attorneys general in California,⁶⁵ the District of Columbia,⁶⁶ Massachusetts,⁶⁷ New York,⁶⁸ and Washington,⁶⁹ as well as by a group of at least forty-seven state attorneys general investigating Facebook for potential antitrust violations.⁷⁰ Similarly, Google settled a complaint with the FTC in August 2019 but has been publicly investigated in the past two years by Arizona,⁷¹ Connecticut and New York (in tandem),⁷² and fifty attorneys general probing the company’s competition practices.⁷³

Because of the increase in the number of investigations targeting the same handful of companies, a former employee who wishes to assist another enforcer with a new case is increasingly likely to find that the new case concerns an old target.

C. TECHNOLOGISTS ACT AS UTILITY PLAYERS

Unlike most other roles at the FTC, every FTC technologist is forced to be a utility player. Although the FTC employs hundreds of attorneys and dozens of economists,⁷⁴ it employs fewer than ten technologists.⁷⁵ The number of technologists has ebbed and flowed and has been as low as only one. Over the past couple decades, however, the technical complexity of U.S. commerce has grown, thereby increasing agency demand for technical expertise. This has an important impact on conflicts. Attorneys and economists can specialize in narrow slices of the agency’s work and focus on a small docket of investigations, but technologists tend to work on a broad set of matters. As a result, for purposes of applying the FTC’s post-employment restrictions, technologists may be more likely than other FTC employees to be consid-

⁶⁴ Press Release, Fed. Trade Comm’n, FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

⁶⁵ Cecilia Kang & David McCabe, *California Sues Facebook for Documents in Privacy Investigation*, N.Y. TIMES (Nov. 6, 2019), <https://www.nytimes.com/2019/11/06/technology/facebook-california-investigation.html>.

⁶⁶ Matthew P. Denn & Amanda Fitzsimmons, *District of Columbia v. Facebook: General Consumer Protection Statute Can Serve as Vehicle for State Attorney General Seeking Redress for Data Privacy Violations*, DLA PIPER (June 12, 2019), <https://www.dlapiper.com/en/us/insights/publications/2019/06/district-of-columbia-v-facebook/>.

⁶⁷ Associated Press, *Facebook Must Provide Info Sought by Massachusetts Attorney General*, BOSTON.COM (Jan. 19, 2020), <https://www.boston.com/news/local-news/2020/01/19/facebook-must-provide-info-sought-by-massachusetts-attorney-general>.

⁶⁸ Makena Kelly, *New York’s Attorney General Is Investigating Facebook After Contact-Scraping Scandal*, THE VERGE (Apr. 25, 2019, 5:15 PM), <https://www.theverge.com/2019/4/25/18516716/new-york-attorney-general-facebook-contact-scraping-letitia-james>.

⁶⁹ Associated Press, *Washington Attorney General Sues Facebook over Campaign Ads*, U.S. NEWS & WORLD REP. (Apr. 14, 2020, 5:47 PM), <https://www.usnews.com/news/best-states/washington/articles/2020-04-14/washington-attorney-general-sues-facebook-over-campaign-ads>.

⁷⁰ Tony Romm, *Forty-Six Attorneys General Have Joined a New York-Led Antitrust Investigation of Facebook*, WASH. POST (Oct. 22, 2019, 1:32 PM), <https://www.washingtonpost.com/technology/2019/10/22/fifty-six-attorneys-general-have-joined-new-york-led-antitrust-investigation-into-facebook/>.

⁷¹ Ali Breland, *Arizona Investigating Google’s Location Tracking: Report*, THE HILL (Sept. 11, 2018, 3:33 PM), <https://thehill.com/policy/technology/406106-arizona-investigating-googles-location-tracking-report>.

⁷² Reuters, *At Least Two U.S. Attorneys General Are Investigating the Google+ Glitch that Exposed Hundreds of Thousands of Users’ Personal Data*, BUS. INSIDER (Oct. 9, 2018, 4:37 PM), <https://www.businessinsider.com/some-us-attorneys-general-are-investigating-google-data-breach-2018-10>.

⁷³ Makena Kelly, *Google Under Antitrust Investigation by 50 Attorneys General*, THE VERGE (Sept. 9, 2019, 2:59 PM), <https://www.theverge.com/2019/9/9/20857440/google-antitrust-investigation-attorneys-general-advertising-search>.

⁷⁴ See *Bureau of Economics Biographies*, Fed. Trade Comm’n, <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-economics/biographies> (last visited May 19, 2021).

⁷⁵ As of May 2019, there were only five technologists at the FTC. See Memorandum from the Comm. on Energy & Commerce Staff to the Subcomm. on Consumer Prot. & Commerce Members and Staff 4 (May 8, 2019), <https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/FTC%20Oversight%20Memo%2050319.pdf>. In May 2021, an FTC official confirmed that the number of technologists on staff is fewer than ten. Notes of conversation on file with authors.

ered to have “participated personally and substantially” in any FTC investigation of a major company.⁷⁶

Technology now pervades nearly every industry the FTC oversees, leading some to refer to it as the “Federal Technology Commission.”⁷⁷ The biggest driver of increasing technical complexity is, of course, the growth of computers and the Internet to their modern-day prevalence.⁷⁸ Personal computers and the Internet are still relatively recent phenomena. In the nineteen years from 1997 to 2016, the percentage of U.S. households with desktop or laptop computers more than doubled.⁷⁹ From 2000 to 2019, the percentage of U.S. adults who used the Internet went from fifty-two percent to ninety percent.⁸⁰ The iPhone was not even introduced until 2007,⁸¹ with the App Store following close behind it, and yet today there are almost two million apps available for download.⁸² E-commerce has simultaneously ballooned over the past two decades.⁸³

Today, technically complex subject matter is often at the center of the agency’s investigations and proceedings. For example, the 2019 Facebook complaint discussed Facebook’s implementation of facial recognition technology;⁸⁴ the 2019 Google/YouTube complaint discussed behavioral advertising;⁸⁵ the 2019 Equifax complaint discussed critical security vulnerabilities and reasonable patch management policies and procedures;⁸⁶ and the 2018 Uber complaint discussed the company’s use of real-time precise geolocation data.⁸⁷

As the role of technology in FTC investigations and enforcement has expanded, the agency has struggled to adjust accordingly, forcing the few available technologists to consult on an outsized portion of agency matters.⁸⁸ Our personal experience bears this out. As technologists for the FTC, we were asked to consult with attorneys working on virtually every case that came before the Division of Privacy and Identity Protection, as well as a number of cases originating in other divisions. In interviews with other former FTC technologists, we heard similar accounts. This means that our potential list of conflicts is much longer than non-technologists who work for the FTC for the same length of time. Nearly every matter involving tech-

⁷⁶ 16 C.F.R. § 4.1(b)(1)(i).

⁷⁷ Brian Fung, *The FTC Was Built 100 Years Ago to Fight Monopolists. Now, It’s Washington’s Most Powerful Technology Cop*, WASH. POST (Sept. 25, 2014, 11:30 AM), <https://www.washingtonpost.com/news/the-switch/wp/2014/09/25/the-ftc-was-built-100-years-ago-to-fight-monopolists-now-its-washingtons-most-powerful-technology-cop/> (quoting Geoffrey Manne, executive director of the International Center for Law and Economics).

⁷⁸ See generally McSweeney, *supra* note 50 (detailing FTC enforcement actions in consumer protection against the backdrop of increasing technological complexity).

⁷⁹ Laptop and desktop computer ownership increased from 36.6 percent in 1997 to 77 percent in 2016. ERIC C. NEWBURGER, U.S. CENSUS BUREAU, COMPUTER USE IN THE UNITED STATES: October 1997, at 1 (1999), <https://www.census.gov/content/dam/Census/library/publications/1999/demo/p20-522.pdf>; CAMILLE RYAN, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2016, at 2 (2018), <https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf>. In 2016, eighty-nine percent of households had a smartphone or computer. RYAN, *supra* note 79, at 1.

⁸⁰ *Internet/Broadband Fact Sheet*, PEW RESEARCH CTR. (June 12, 2019), <https://www.pewresearch.org/internet/fact-sheet/internet-broadband/>.

⁸¹ Lisa Eadicicco, *This Is Why the iPhone Upended the Tech Industry*, TIME (June 29, 2017, 7:00 AM), <https://time.com/4837176/iphone-10th-anniversary/>.

⁸² Sam Costello, *How Many Apps Are in the App Store?*, LIFEWIRE, <https://www.lifewire.com/how-many-apps-in-app-store-2000252> (last updated Feb. 24, 2020).

⁸³ U.S. retail e-commerce sales were estimated at \$5.3 billion in the fourth quarter of 1999, when the U.S. Census Bureau first began reporting e-commerce statistics, representing 0.64 percent of total retail sales. Press Release, U.S. Census Bureau, Retail E-Commerce Sales for the Fourth Quarter 1999 Reach \$5.3 Billion, Census Bureau Reports (Mar. 2, 2000), <https://www2.census.gov/retail/releases/historical/ecom/99q4.pdf>. By the first quarter of 2020, retail e-commerce sales had ballooned to \$160.3 billion, representing 11.8 percent of total retail sales. Press Release, U.S. Census Bureau, Quarterly Retail E-Commerce Sales: 1st Quarter 2020 (May 19, 2020), <https://www2.census.gov/retail/releases/historical/ecom/20q1.pdf>.

⁸⁴ Complaint for Civil Penalties, Injunction, and Other Relief at 6, 39–42, *United States v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C. July 14, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

⁸⁵ Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 4, 7–9, *Fed. Trade Comm’n v. Google LLC*, No. 1:19-cv-2642 (D.D.C. Sept. 6, 2019), https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_revised_complaint.pdf.

⁸⁶ Complaint for Permanent Injunction and Other Relief at 6, 8–14, *Fed. Trade Comm’n v. Equifax Inc.*, No. 1:19-mi-99999–UNA (N.D. Ga. July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf.

⁸⁷ Complaint at 2, *Uber Technologies, Inc.*, No. C–4662 (Fed. Trade Comm’n Oct. 26, 2018), https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_complaint.pdf.

⁸⁸ This has been our experience, as well as the experience of several people we interviewed. Contact authors for information on interviews.

nology during our tenure crossed our desks, even if many of those interactions were fleeting and insubstantial. Still, our list of potential conflicts encompasses nearly everything involving complex information technology during our employment.

The general dearth of technical experts at the FTC reflects the agency's dearth of staff more broadly. Much of the scrutiny the agency exacts on technology companies is facilitated by staff working on privacy and data security, of which the FTC has only about forty.⁸⁹ In contrast, the United Kingdom has more than five hundred people working in its Information Commissioner's office,⁹⁰ and Ireland's Data Protection Commissioner has over 130 employees.⁹¹ As far as technologists are concerned, while the FTC has between five and nine technologists,⁹² Germany—a country with one-fourth the population of the United States—has 101 technology specialists working with its data protection authorities.⁹³ While such a high number is unusual, other European countries nevertheless have drastically more technologists than the United States; Spain has thirty-six, France has twenty-eight, and the United Kingdom has twenty-two.⁹⁴

The dearth of FTC technologists is also evident in comparison to the large population of economists employed by the FTC. The FTC's website currently lists approximately 80 staff in the Bureau of Economics.⁹⁵ This list does not include economists who serve in other roles, such as staff advisors for Commissioners.⁹⁶ With dozens of economists and supporting analysts on staff, it is neither necessary nor feasible to ask any individual economist to take on such a broad portfolio of matters that might serve as a future potential conflict of interest.

D. LENGTHY AND BROAD CONSENT DECREES

Another possible contributor to the FTC's broad application of conflicts rules for technologists is the agency's practice of establishing broad, twenty-year settlements with parties presumed to be in violation of § 5 of the FTC Act.⁹⁷ This would not necessarily pose a problem if the FTC understood that the "proceeding or investigation" in a conflict of interest analysis under § 4.1(b) of the agency's rules should be the specific facts that gave rise to the twenty-year settlement. But if the rules are instead read broadly—too broadly in our view—to encompass "this company and privacy" or "this company and security," the twenty-year term serves as a two-decades-long restraint on future work for former employees. In combination with the fact that companies—especially technology companies—are bigger and more horizontally diversified than they were in the past,⁹⁸ broad and lengthy consent decrees dramatically limit the ability of former FTC staff to work on issues related to technology companies for a period that may cover half a person's professional career.

The FTC has existing consent decrees that will endure many years into the future with a large number of major companies. For example, from past cases, the agency

⁸⁹ Harper Neidig, *FTC Says It Only Has 40 Employees Overseeing Privacy and Data Security*, THE HILL (Apr. 3, 2019, 11:01 AM), <https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security>.

⁹⁰ History of the ICO, INFO. COMM'R'S OFFICE, <https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/> (last visited Aug. 23, 2020).

⁹¹ Peter Hamilton, *Data Commissioner to Look for More Staff and Funding*, IRISH TIMES (Mar. 7, 2019, 1:50 PM), <https://www.irishtimes.com/business/technology/data-commissioner-to-look-for-more-staff-and-funding-1.3817791>.

⁹² See Breland, *supra* note 71.

⁹³ JOHNNY RYAN, BRAVE, EUROPE'S GOVERNMENTS ARE FAILING THE GDPR 4 (2020), <https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf>.

⁹⁴ *Id.*

⁹⁵ See Bureau of Economics Biographies, *supra* note 74.

⁹⁶ See FED. TRADE COMM'N, FEDERAL TRADE COMMISSION ORGANIZATION DIRECTORY 2, https://www.ftc.gov/system/files/attachments/contact-federal-trade-commission/ftc_org_directory_8-8-2019.pdf (last updated Aug. 8, 2019) (listing an "Economic Advisor" for Chairman Joseph J. Simons).

⁹⁷ See *Legislative Hearing on 17 FTC Bills: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 5 (2016) (statement of David C. Vladeck, Professor, Georgetown University Law Center), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/05.24.16_Testimony_Vladeck-CMT-LegHrg-17-FTC-Bills-20160524.pdf ("[T]he Commission has for decades generally insisted on twenty year [sic] orders."); *id.* at 6 ("[M]ost [data security cases] were resolved with twenty-year consent decrees."); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 613–14 (2014) (citing twenty years as a common duration for FTC's privacy and security audits, while also noting variation among the orders); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2297 (2015) ("While the FTC does not enter into a twenty-year consent order with every company it files a privacy-related complaint against, this burdensome timescale is the most common duration for such agreements.");

⁹⁸ See discussion in *supra* Section III.C.

has settlement provisions that will persist with Facebook until 2039,⁹⁹ with Apple until 2034,¹⁰⁰ with Google until 2031,¹⁰¹ with Google/YouTube until 2029,¹⁰² with Twitter until 2030,¹⁰³ and with PayPal until 2038.¹⁰⁴

The consent decrees often include provisions that require special behavior, oversight, or reporting with respect to a broad range of activities. For example, consent decrees negotiated as part of privacy and data security cases commonly require parties to commit to not misrepresent their privacy or security practices,¹⁰⁵ obtain express consent from consumers with respect to certain data practices,¹⁰⁶ adopt privacy or security programs incorporating certain specific practices,¹⁰⁷ produce regular privacy or security reports that meet outlined standards,¹⁰⁸ and make certain documents available to the FTC upon request.¹⁰⁹

Because the term of the agreements is long and the scope broad, former employees may find that if they worked on or saw documents related to an investigation of a company that later settled with the FTC, future work relating generally to the data practices of that same company is then essentially off-limits for the lengthy term of the agreement. Even investigations into products or services that *did not yet exist* at the time can then be construed as the “same proceeding or investigation” under the agency’s rules restricting post-employment activities.¹¹⁰

E. RISK-AVERSE AGENCY CULTURE

When we interviewed former FTC employees, they generally agreed that another cause of the agency’s broad application of post-employment conflicts rules is a cultural inclination toward risk-aversion at the agency.¹¹¹ In particular, interviewees

⁹⁹ Stipulated Order for Civil Penalty, Monetary Judgement, and Injunctive Relief at Attachment A at 20, *United States v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf [hereinafter “FTC Facebook Order 2019”] (“This Order will terminate 20 years from the date of its issuance, or 20 years from the most recent date that the United States of the Commission files a complaint”).

¹⁰⁰ Decision and Order at 6, *Apple Inc.*, No. C-4444 (Fed. Trade Comm’n Mar. 25, 2014), <https://www.ftc.gov/system/files/documents/cases/140327apple.pdf> [hereinafter “FTC Apple Order 2014”] (“This order will terminate on March 25, 2034, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint”).

¹⁰¹ Agreement Containing Consent Order at 7, *Google Inc.*, No. 102316 (Fed. Trade Comm’n 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf> [hereinafter “FTC Google Order 2011”] (“This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Commission files a complaint”).

¹⁰² Stipulated Order for Permanent Injunction and Civil Penalty Judgement at 16, *Fed. Trade Comm’n v. Google LLC*, No. 1:19-cv-02642 (D.D.C. Sept. 4, 2019), https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf [hereinafter “FTC Google/YouTube Order 2019”] (“For ten (10) years after entry of this Order, each Defendant must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in”).

¹⁰³ Agreement Containing Consent Order at 6, *Twitter, Inc.*, No. 0923093 (Fed. Trade Comm’n 2010), <https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twitteragree.pdf> [hereinafter “FTC Twitter Order 2010”] (“This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Commission files a complaint”).

¹⁰⁴ Decision and Order at 7, *Paypal, Inc.*, No. C-4651 (Fed. Trade Comm’n May 23, 2018), https://www.ftc.gov/system/files/documents/cases/1623102-c4651_paypal_venmo_decision_and_order_final_5-24-18.pdf [hereinafter “FTC PayPal Order 2018”] (“Respondent must create certain records for 20 years after the issuance date of the Order.”).

¹⁰⁵ See, e.g., FTC Facebook Order 2019, *supra* note 99, at 5; FTC PayPal Order 2018, *supra* note 104, at 3; FTC Google Order 2011, *supra* note 101, at 3–4; FTC Twitter Order 2010, *supra* note 103, at 3.

¹⁰⁶ See, e.g., FTC Facebook Order 2019, *supra* note 99, at 5–6; FTC Google Order 2011, *supra* note 101, at 4.

¹⁰⁷ See, e.g., FTC Facebook Order 2019, *supra* note 99, at 6–12; FTC Google Order 2011, *supra* note 101, at 4–5; FTC Twitter Order 2010, *supra* note 103, at 3–4.

¹⁰⁸ See, e.g., FTC Facebook Order 2019, *supra* note 99, at 12–14; FTC PayPal Order 2018, *supra* note 104, at 5–6; FTC Google Order 2011, *supra* note 101, at 5–6; FTC Twitter Order 2010, *supra* note 103, at 4–5.

¹⁰⁹ See, e.g., FTC Facebook Order 2019, *supra* note 99, at 20; FTC PayPal Order 2018, *supra* note 104, at 8; FTC Google Order 2011, *supra* note 101, at 6; FTC Twitter Order 2010, *supra* note 103, at 5–6.

¹¹⁰ 16 C.F.R. § 4.1(b)(1)(i).

¹¹¹ Interviews, *supra* note 88; see also Nicholas Confessore & Cecilia Kang, *Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites*, N.Y. TIMES (Dec. 30, 2018), <https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html> (“In more than 40 interviews, former and current F.T.C. officials, lawmakers, Capitol Hill staff members, and consumer advocates said that as evidence of abuses has piled up against tech companies, the F.T.C. has been too cautious.”).

stated that there is a widespread concern about heavy congressional criticism within the agency.¹¹² This is viewed as a motivating factor for a number of agency considerations. Many interviewees stated a belief that the agency's extreme caution harkens back to the 1970s when, in what is known as "KidVid," the agency attempted to ban television ads for junk food directed at children—a move perceived by a congressional majority as regulatory overreach.¹¹³ In response, Congress limited the agency's authority and withdrew its funding.¹¹⁴ Many believe that the agency continues to tread lightly today out of a lingering fear of congressional backlash, an assessment echoed by our interviewees. Applying this approach to conflicts questions, the agency may reasonably calculate that there are few or no downsides to OGC rejecting a former employee's clearance request.

In contrast, granting a former employee's clearance request—especially when it concerns a major company or highly visible matter—could provide fodder for a company under the scrutiny of the FTC to attempt to drum up criticism of the agency. This is not an unfounded concern; in response to unwanted FTC investigation, companies have attempted all manner of interference strategies throughout the agency's history. For example, in 1918 when the FTC issued a report documenting the predatory and collusive practices of meatpackers and calling for the nationalization of certain components of the industry, the agency was roundly attacked.¹¹⁵ The U.S. Chamber of Commerce and the New York Times Editorial Board called for the agency to be "cured of its present bolshevist and propagandist tendencies,"¹¹⁶ and were echoed by Senator James Watson when he specifically targeted the FTC's Chicago field office as a "spawning ground of sovietism."¹¹⁷ In response, the agency investigated, cleared of wrongdoing, but ultimately still fired eleven of the employees who worked on the report, and Congress removed the agency's oversight of meatpackers, awarding this jurisdiction instead to the more industry-friendly Department of Agriculture.¹¹⁸ Sixty years later in KidVid, when the agency considered children's advertising rules, advertisers devoted the equivalent of one-fourth of the agency's budget at the time to lobbying and public relations efforts against the rules, while advertising trade associations petitioned the FTC to compel Chair Michael Perschuk to recuse himself based on his prior statements about the regulation of children's advertising.¹¹⁹ When Perschuk initially refused, the advertisers sued, won, and lost on

¹¹² Interviews, *supra* note 88.

¹¹³ See CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 60–66 (2016) (describing the KidVid controversy, the ensuing fallout, and the impact on the FTC's enforcement approach); Confessore & Kang, *supra* note 111 ("The F.T.C. is haunted, for example, by a clash with Congress in the 1980s over an attempt by the agency to ban television ads for junk food directed at children, known as 'KidVid.' . . . Fears that Congress could again cripple the F.T.C. have made some career lawyers reluctant to take on politically sensitive cases, according to current and former employees, speaking about their experiences during the Trump and Obama administrations."). In one memorable example of a culture of severe sensitivity to congressional censure at the agency, an interviewee described briefing their superiors on research that websites were using JavaScript code that could surreptitiously dig through a user's browser and access the sites they had visited. (Please contact authors for information on interviews.) The most heavily trafficked site that was engaging in that practice belonged to a pornography website. *Id.* The interviewee was informed that the agency would not investigate the pornography company because the FTC did not want to run the risk of being perceived as "protecting the privacy of people who watch pornography." *Id.* While no other interviewees provided similarly colorful examples to illustrate the point, this example is representative of the risk-averse culture described by the other former FTC employees.

¹¹⁴ Hoofnagle, *supra* note 113, at 65 (describing the FTC Improvement Act of 1980, which passed in response to the KidVid controversy, implemented a Congressional veto of Agency action, limited the Agency's rule-making authority, and temporarily expunged funding).

¹¹⁵ Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U.L. REV. 431, 467 (2021). The practices described in the report also provided the basis for a subsequent criminal suit by the Attorney General.

¹¹⁶ Editorial, *The Trade Commission*, N.Y. TIMES, Sept. 3, 1918, at 10, available at https://timesmachine.nytimes.com/timesmachine/1918/09/03/97024087.pdf?pdf_redirect=true&ip=0.

¹¹⁷ Paul A. Pautler, *A Brief History of the FTC's Bureau of Economics: Reports, Mergers, and Information Regulation*, 46 REV. INDUS. ORG. 59, 64 n.13 (2015).

¹¹⁸ *Id.* (noting that the employees were "cleared of wrongdoing" and that their firing was "presumably to placate Senator Watson"); Hoofnagle, *supra* note 113, at 24–25 (recounting the episode and characterizing the Department of Agriculture as "friendlier" to the meatpackers than the FTC).

¹¹⁹ Herrine, *supra* note 115, at 503 ("With General Mills and Bristol-Myers in the lead and 'Washington super-lobbyist Tommy Boggs' coordinating (and rumors of the tobacco lobby contributing substantially), a 'war chest' of \$30 million was raised to 'Stop the FTC' and KidVid in particular."); *id.* at 506–07 (detailing The Association of National Advertisers, Inc., the American Association of Advertising Agencies, the American Advertising Federation, and the Toy Manufacturers of America, Inc.'s demands that Perschuk recuse himself for conflict of interest).

Continued

appeal; nevertheless, Perschuk eventually recused himself voluntarily to shield the rulemaking from further corruption accusations.¹²⁰ These episodes provide support for fears of corporate retaliation: when it comes to companies attempting to avoid profit-narrowing regulation, some will not hesitate to work the referees, and many of those will be rewarded with the calls they sought.

Indeed, we know of at least two instances when the agency acted on outside claims of conflict or bias that seemed exceptionally weak on their face, and for which it is difficult to explain the agency's responses as anything other than extreme risk aversion. One former technologist we interviewed publicly criticized a large technology company prior to his employment by the agency.¹²¹ When the company filed a complaint with the FTC regarding the employee's participation in investigations of the company, the FTC removed the employee from the investigation and precluded him from working on any investigation of that company for the rest of his employment at the FTC. In another case, a large technology company complained to the FTC when a member of an FTC technologist's Ph.D. dissertation committee filed a public request for the agency to investigate that company. The request was based entirely on publicly available information but, because the company complained that the employee was somehow conflicted, the FTC prohibited the employee from working on any investigations of that company. As a result, an important investigation of the company was conducted without the support of any FTC technologist for several months.

The agency's attempts to inoculate itself from charges of bias by industry are likely to fail because opportunistic companies raise such charges even when there is no reasonable basis for them. Nevertheless, a deep-seated agency culture of prudence—and a history of successful corporate interference—leads the agency to reflexively shy away from even the suggestion of possible conflict.

F. POSSIBLE POLITICAL CONFLICT BETWEEN FTC AND STATE ATTORNEYS GENERAL

It is also possible that perceived political conflict may contribute to the overly broad application of post-employment conflict restrictions to FTC technologists. To be clear, the FTC often works closely with state attorneys general, including in investigations into the practices of technology companies.¹²² For example, in 2012, the FTC and dozens of state attorneys general coordinated on cases brought against Google for its privacy policy practices.¹²³ Even though the state enforcers pressed arguably more aggressive theories than the FTC pursued in its investigation, FTC Commissioner Julie Brill praised the settlement extracted by the states.¹²⁴

Our interviewees downplayed the possibility of rivalry between the FTC and the states as playing a significant role in the FTC's application of post-employment restrictions. Many of our respondents thought it unlikely that perceived political conflict plays a meaningful role driving the FTC's broad application of post-employment conflict rules. Nevertheless, this is a possibility worth exploring.

Although the state attorneys general and the FTC frequently are well aligned, their respective goals and approaches sometimes diverge. A 2013 investigation of Google, regarding the company bypassing privacy settings in the Safari browser, led the FTC to enter a settlement with Google that required no limits on Google's future behavior.¹²⁵ State attorneys general declined the FTC's invitation to join the consent decree and continued to press a parallel case that led, arguably, to tougher restrictions on Google's conduct.¹²⁶

due to his “public statements concerning regulation of children’s advertising that demonstrated prejudgment of specific factual issues sufficient to preclude his ability to serve as an impartial arbiter”) (citing *Ass’n of Nat’l Advertisers, Inc. v. FTC*, 627 F.2d 1151, 1155 (D.C. Cir. 1979)).

¹²⁰ Herrine, *supra* note 115, at 503.

¹²¹ Contact authors for more information.

¹²² Paul M. Schwartz, *The Value of Privacy Federalism*, in *SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES* 324 (Beate Roessler & Dorota Mokrosinska eds., 2015) (“When Congress enacts privacy law, it generally allows the states space for further action.”); Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 791–94 (2016) (“Attorneys general have enjoyed a synergistic relationship with Federal agencies working on privacy and data security issues.”); Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 LEWIS & CLARK L. REV. 595, 621–22 (2016) (“[T]he state attorneys general have not only coordinated their actions horizontally but have also joined efforts with the FTC.”).

¹²³ Citron, *supra* note 122, at 793.

¹²⁴ *Id.*; Letter from Twenty-three Att’y’s Gen. to Larry Page, Chief Exec. Officer, Google, Inc. (Feb. 22, 2012), <https://epic.org/privacy/google/20120222-Google-Privacy-Policy-Final.pdf>.

¹²⁵ Citron, *supra* note 122, at 770 (citing Press Release, Fed. Trade Comm’n, Google Will Pay \$22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple’s Safari Internet Browser (Aug. 9, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>).

¹²⁶ *Id.*

There are reasons to believe that some amount of competitiveness exists between these entities. In many ways, the FTC has become the *de facto* privacy and technology regulator in the United States, even though, outside of sectoral laws like the Children's Online Privacy Protection Act (COPPA) and the Fair Credit Reporting Act (FCRA), there is currently no comprehensive Federal privacy law.¹²⁷ The FTC benefits from the appearance that it is the primary and most powerful enforcer of fair trade practices in the United States because, when a regulator has a reputation as being toothless, companies subject to their jurisdiction have no incentive to comply with the relevant rules. As a result, the FTC sometimes competes with state attorneys general when enforcing high-profile cases. When state enforcement agencies investigate and impose stronger perceived penalties on companies that the FTC has already investigated, charged, and settled, this could undermine the FTC's status as supreme enforcer.¹²⁸

The experiences of one interviewee who worked on consumer protection investigations with a state attorney general's office speak to the occasional tensions between the FTC and state attorneys general. The interviewee hypothesized that in certain, high-profile cases, the FTC's willingness to allow the former employee to consult on the state attorney general's case was hindered by the agency's interest in public credit for tackling certain cases. The interviewee hypothesized that the agency's desire for public credit was responsible for the friction in that particular case because the interviewee had not encountered similar problems when working with FTC officials on previous lower-level cases. The interviewee explained that in response to a request for clearance to work with state AGs on a high-profile matter, the FTC denied clearance for the interviewee unless the interviewee was willing to work as an unpaid FTC employee and allow the FTC to mediate their recommendations to the state agencies.¹²⁹ Indeed, there is good reason for FTC staff to seek public credit for its enforcement efforts. In recent years, the FTC has been lambasted by a range of critics for its failure to take strong, decisive action to rein in unfair and deceptive trade practices.¹³⁰ Even the agency's record-breaking five-billion-dollar settlement with Facebook drew widespread criticism that it was simply not enough.¹³¹

¹²⁷ Solove & Hartzog, *supra* note 97, at 600–08.

¹²⁸ See Justin Brookman, *State Attorneys General: Evading Privacy Settings Is Illegal*, CTR. FOR DEMOCRACY & TECH. (Nov. 20, 2013), <https://cdt.org/insights/state-attorneys-general-evading-privacy-settings-is-illegal/> (pointing out that the 2013 settlement by state attorneys general with Google was “considerably more expansive than the FTC’s,” and arguing that “it’s heartening to see states increasingly take action to protect consumer privacy”); Citron, *supra* note 122, at 756 n.42 (“In important areas, [state attorneys general (AG)] have set privacy policy in the absence of Federal norms; in others, they have pressed the FTC to offer greater privacy protections to consumers than those afforded by Federal agencies. In the near future, there may be more aggressive state AG privacy and data security enforcement than enforcement activity at the Federal level.”).

¹²⁹ E-mail from Alternate Designated Agency Ethics Official, Office of the General Counsel, Federal Trade Commission, to one of the authors (Mar. 07, 2019, 07:54 PST) (on file with authors).

¹³⁰ See, e.g., Hearing on Oversight of the Federal Trade Commission: Strengthening Protections for Americans’ Privacy and Data Security Before House of Representatives Subcommittee on Consumer Protection and Commerce of the House Committee on Energy and Commerce, 116th Cong. 1 (May 8, 2019) (opening statement of Frank Pallone, Jr., Chairman, Comm. on Energy & Commerce), <https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/0508%20FP%20FTC%20Oversight%20Hrg%20Opening%20Remarks.pdf> (claiming the FTC “can dodo[es] little more than give a slap on the wrist to companies the first time they violate the law”); Emily Birnbaum, *GOP Senator Scolds FTC for ‘Toothless’ Response to Privacy Scandals*, THE HILL (Mar. 11, 2019, 1:41 PM), <https://thehill.com/policy/technology/433514-gop-senator-ftc-response-to-privacy-scandals-has-been-toothless>; Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (June 28, 2012, 6:30 AM), <https://www.wired.com/2012/06/ftc-fail/> (calling the FTC “low-tech, defensive, [and] toothless”).

¹³¹ See, e.g., Devin Coldewey, *9 Reasons the Facebook FTC Settlement Is a Joke*, TECHCRUNCH (July 24, 2019, 8:01 PM), <https://techcrunch.com/2019/07/24/9-reasons-the-facebook-ftc-settlement-is-a-joke/>; Editorial Board, *Opinion, A \$5 Billion Fine for Facebook Won’t Fix Privacy*, N.Y. TIMES (July 25, 2019), <https://www.nytimes.com/2019/07/25/opinion/facebook-fine-5-billion.html>; Nilay Patel, *Facebook’s \$5 Billion FTC Fine Is an Embarrassing Joke*, THE VERGE (July 12, 2019, 9:05 PM), <https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke>; Adam Schwartz, *The FTC-Facebook Settlement Does Too Little to Protect Your Privacy*, ELEC. FRONTIER FOUND. (July 24, 2019), <https://www.eff.org/deeplinks/2019/07/ftc-facebook-settlement-does-too-little-protect-your-privacy>; Siva Vaidhyanathan, *Billion-Dollar Fines Can’t Stop Google and Facebook. That’s Peanuts for Them*, GUARDIAN (July 26, 2019, 6:00 AM), <https://www.theguardian.com/commentisfree/2019/jul/26/google-facebook-regulation-ftc-settlement>; Press Release, H. Comm. on Energy & Commerce, *Pallone Statement on the FTC’s Facebook Settlement* (July 24, 2019), <https://energycommerce.house.gov/newsroom/>

Some critics have gone so far as to argue that what they consider to be the agency's too-weak enforcement efforts provide support to further constrain the agency's authority. Indeed, a number of privacy advocates have called for Congress to create a new data protection authority to counteract the FTC's failures and hold technology companies accountable.¹³² Senator Gillibrand,¹³³ Senator Brown,¹³⁴ and Representatives Lofgren and Eshoo¹³⁵ heeded that call by offering legislation that would establish a new data protection agency in the United States.

The FTC could be concerned that if state attorneys general were to frequently pursue additional enforcement action against companies for practices that have already been the subject of FTC settlements, companies would have less of an incentive to agree to truly burdensome conditions when they are brought to the settlement negotiation table over alleged violations. It is not unusual for the FTC to release any claims it may have against the subjects of its enforcement actions as part of the negotiated settlement.¹³⁶ If a company caught violating the FTC Act believed it was likely to just be sued again for the same behavior by another enforcer, then the FTC's avowal to release any claims related to the violation would have little value.

IV. IMPLICATIONS FOR AGENCY EFFICACY

As this Article has noted throughout, the broad application of the conflict rules undermines their purpose and the FTC's ability to fulfill its competition and consumer protection mission. The FTC is making it less attractive for technologists to work at the agency by disproportionately limiting the work they are able to do, including when the matters former employees are being precluded from participating in create neither an actual conflict nor the appearance of it. Unwieldy and unpredictable post-employment constraints will make it even less attractive, or frankly feasible, for technologists to work for the FTC than it already is, raising exactly the concerns that Congress has repeatedly noted when revising §207.¹³⁷

This overbroad application of the FTC's rules also undermines the agency's broader mission of consumer protection by inhibiting other consumer protection actors, such as state attorneys general, from gaining the expertise to adequately seek rem-

press-releases/pallone-statement-on-the-ftc-s-facebook-settlement ("While \$5 billion is a record fine for the FTC, monetary damages are not enough.").

¹³² See, e.g., Caitriona Fitzgerald & Mary Stone Ross, *Now Is the Time for a U.S. Data Protection Agency*, THE HILL (Feb. 21, 2020, 9:30 AM), <https://thehill.com/blogs/congress-blog/politics/483997-now-is-the-time-for-a-us-data-protection-agency> ("Congress needs to create a Data Protection Agency because the Federal Trade Commission is failing to protect privacy."); PRIVACY & DIG. RIGHTS FOR ALL COAL., THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL RIGHTS IN THE UNITED STATES, <https://www.citizen.org/up-content/uploads/migration/privacy-and-digital-rights-for-all-framework.pdf>; The U.S. Urgently Needs a Data Protection Agency, ELEC. PRIVACY INFO. CTR., <https://epic.org/dpa/>; see also Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N.Y. TIMES (Nov. 2, 2019), <https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html> (describing critiques of the FTC and proposals for a new data protection agency).

¹³³ Press Release, Kirsten Gillibrand: U.S. Sen. for N.Y., Confronting a Data Privacy Crisis, Gillibrand Announces Landmark Legislation to Create a Data Protection Agency (Feb. 13, 2020), <https://www.gillibrand.senate.gov/news/press/release/confronting-a-data-privacy-crisis-gillibrand-announces-landmark-legislation-to-create-a-data-protection-agency>.

¹³⁴ Press Release, Sherrod Brown: U.S. Sen. for Ohio, Brown Releases New Proposal That Would Protect Consumers' Privacy from Bad Actors (June 18, 2020), <https://www.brown.senate.gov/newsroom/press/release/brown-proposal-protect-consumers-privacy>.

¹³⁵ Press Release, Congresswoman Anna G. Eshoo, Eshoo & Lofgren Introduce the Online Privacy Act (Nov. 5, 2019), <https://eshoo.house.gov/media/press-releases/eshoo-lofgren-introduce-online-privacy-act>.

¹³⁶ See, e.g., FTC Facebook Order 2019, *supra* note 99; [Proposed] Stipulated Revised Order for Permanent Injunction and Equitable Monetary Relief at 17, Fed. Trade Comm'n v. Cephalon, Inc., No. 2:08-cv-2141-MSG (E.D. Pa. Feb. 19, 2019), <https://www.ftc.gov/system/files/documents/cases/teva-proposed-stipulated-revised-order.pdf> ("The Commission and the Cephalon Parties stipulate that upon entry of the Revised Order, the Commission and the Cephalon Parties each release the other from any and all claims, causes of actions and demands"); Stipulation at 2, United States v. Okumus, No. 1:17-cv-00104 (D.D.C. Jan. 17, 2017), <https://www.ftc.gov/system/files/documents/cases/170117okumus-stipulation-filed.pdf> ("The entry of the Final Judgment in accordance with this Stipulation settles, discharges, and releases any and all claims of Plaintiff for civil penalties and equitable relief pursuant to Section 7A(g)(1) of the Clayton Act, 15 U.S.C. § 18a(g)(1) . . . in connection with Defendant's acquisitions of voting securities of Web.com Group, Inc. from 2014 through 2016."); Stipulated Order for Permanent Injunction and Monetary Judgement at 7, Fed. Trade Comm'n v. Hold Billing Services, Ltd., No. 5:98-cv-006292, (W.D. Tex. May 4, 2016), <https://www.ftc.gov/system/files/documents/cases/160504holdbillingstip.pdf> ("Upon entry of this Stipulated Order, the FTC releases [Defendant] from any and all Claims that it may have stemming from charges to consumers' landline telephone bills through or on behalf of any third-party seller of Enhanced Services.").

¹³⁷ *Supra* notes 13, 17.

edies in areas the FTC itself was unable to obtain. For example, many organizations criticized the five-billion-dollar settlement with Facebook because the settlement includes very little in the way of injunctions to restrict the company's future practices with regards to privacy harm of third-party companies, like Cambridge Analytica.¹³⁸ In fact, the final settlement also precludes Facebook, its executives, and its board of directors from being held responsible for "any and all claims" prior to the settlement date.¹³⁹ Two FTC Commissioners criticized this point, and one implied the existence of other ongoing investigations into the company that were released as a part of the settlement.¹⁴⁰ In addition, private plaintiffs already face steep hurdles to getting their privacy violations redressed due to years of judicial hostility toward privacy rights.¹⁴¹ Making it harder for private plaintiffs to find and retain technology experts will make the already minimal utility of courts to vindicate privacy rights less meaningful still.

Overbroad application even limits the efficacy of the few technologists the agency does employ. In the interviews we conducted, we heard from former employees who had recused themselves from working on certain cases for fear of being broadly precluded from ever working on a related matter once they left the agency, one citing market consolidation as the justification. As such, concerns of post-employment conflict checks are likely chilling the freedom that current FTC employees have to work on certain investigations while at the agency. This corrodes the agency's effectiveness given how few technologists it employs already. With the agency's current volume of technologists, if even one technologist declines to work on cases involving Facebook or Google, for example, the agency loses a significant fraction of its available technological expertise—expertise that it cannot afford to lose.

The FTC is taking the population of employees that it has the hardest time recruiting and making it disproportionately even less attractive for them to work there. Technologists are subject to potential conflicts far more broadly than employees in other disciplines, even though technologists are much harder for the agency to locate and retain than attorneys and economists.¹⁴² An entry-level engineer's compensation at Facebook with no post-collegiate work experience can reach \$166,000 and up to \$189,000 at Google in 2019, while senior staff roles at the FTC can only make up to around \$170,000.¹⁴³ This difference in potential salary in conjunction with the broad and opaque application of the conflict rules render it even less appealing for technologists to work at the FTC. Not only are the conflicts rules making it harder for the agency to recruit and retain the population of employees

¹³⁸ See, e.g., *supra* note 131 and sources cited therein.

¹³⁹ FTC Facebook Order 2019, *supra* note 99, at 1, *United States v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

¹⁴⁰ See OFFICE OF COMM'R ROHIT CHOPRA, FED. TRADE COMM'N, COMM'N FILE NO. 1823109, DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA: IN RE FACEBOOK, INC. 17–18, (2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf ("This means that the proposed release not only shields Facebook from 'known' (an undefined term) Section 5 claims, but also 'known' claims under COPPA and other statutes. Given persistent questions about Facebook's compliance with these statutes, the Commission should be transparent about which claims are being released—even if they are being released because they are seen as lacking viability."); OFFICE OF COMM'R REBECCA KELLY SLAUGHTER, FED. TRADE COMM'N, DISSENTING STATEMENT OF COMMISSIONER REBECCA KELLY SLAUGHTER: IN THE MATTER OF FTC VS. FACEBOOK 14 (2019), https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf (objecting "strenuously" to the settlement's liability exculpation for Facebook's executives and calling the scope of the liability release "unjustified by our investigation and unsupported by either precedent or sound public policy").

¹⁴¹ Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 356–65 (2015) (describing how courts have made it more and more difficult for privacy plaintiffs to receive redress through artificially narrow definitions of Article III standing and injury, and an expansive approach to First Amendment rights and the rights of corporations); Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 575–77 (2017) (describing courts' response to privacy litigants as "busily constructing classes of consumers who lack remedies before the law").

¹⁴² Different factors, such as advance planning and unchanging subject matter, influence why non-technologists are easier for the agency to find and retain. For example, the Bureau of Economics at the FTC was proactive in its creation rather than reactive; that is, it was created all at once with many staff with the objective of changing the agency's focus, as opposed to bit by bit in reaction to subject matter changing beyond the agency's control.

¹⁴³ Adam Janofsky & Matt Drange, *We Counted the FTC Employees who Moved Over to Tech. Is Reform Needed?*, PROTOCOL (Mar. 9, 2020), <https://www.protocol.com/ftc-tech-hawley-revolving-door/>; Kif Leswing, *Here's How Big Tech Companies Like Google and Facebook Set Salaries for Software Engineers*, CNBC (June 15, 2019, 9:30 AM), <https://www.cnbc.com/2019/06/14/how-much-google-facebook-other-tech-giants-pay-software-engineers.html>.

it needs most,¹⁴⁴ they seem fairly ineffective at reducing the revolving door problems for non-technologist employees and senior leadership.¹⁴⁵

In almost cruel irony, the lack of competition among the technology companies subject to the FTC's jurisdiction further hampers its ability to enforce antitrust laws. The technology companies that the FTC investigates, like Apple, Amazon, Facebook, and Google, are frequently repeat players.¹⁴⁶ The size of these companies and the range of markets they have inserted themselves into makes overlap inevitable. When the FTC prohibits an employee from working on matters related to one technology company, that often means that the employee will be forbidden from working on a whole host of investigations across a wide gamut of sectors.¹⁴⁷ The lack of competition in the technology sector means that the agency's broad enforcement of the conflicts rules will significantly undercut its efforts to fulfil its consumer protection and competition missions.

Meanwhile, the collateral effects of the FTC's overreaction hamper its ability to oversee those companies effectively. The agency simply does not employ enough technologists to be able to sideline them every time a subject or potential subject of investigation files a bad-faith complaint. As of 2019, the FTC only employed five full-time technologists in total, for an agency that oversees digital consumer protection issues for a nation of 330 million people and handles a range of other issues beyond privacy, security, and digital competition.¹⁴⁸ The FTC's lack of sufficient

¹⁴⁴ See generally McSweeney, *supra* note 50.

¹⁴⁵ See generally *id.*; see also Rick Claypool, *The FTC's Big Tech Revolving Door Problem*, PUB. CITIZEN (May 23, 2019), <https://www.citizen.org/article/ftc-big-tech-revolving-door-problem-report>.

¹⁴⁶ See, e.g., Agreement Containing Consent Order, Facebook, Inc., No. 0923184 (Fed. Trade Comm'n Nov. 29, 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf> (2011 Facebook consent order); Press Release, Fed. Trade Comm'n, Apple Inc. Will Provide Full Consumer Refunds of At Least \$32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent (Jan. 15, 2014), <https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million> (2014 Apple settlement); Press Release, Fed. Trade Comm'n, Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns in the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search (Jan. 3, 2013), <https://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc> (2013 Google-specific antitrust settlement); Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> (2019 Google and YouTube settlement); Press Release, Fed. Trade Comm'n, Google Will Pay \$22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> (2012 Google settlement); Facebook, Inc., *In the Matter of*, FED. TRADE COMM'N, <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc> (last updated Apr. 28, 2020) (2019 Facebook settlement); Lesley Fair, *FTC Settlement with Amazon Yields \$70 Million for Consumers, Advice for Business*, FED. TRADE COMM'N: BUS. BLOG (May 30, 2017, 12:07 PM), <https://www.ftc.gov/news-events/blogs/business-blog/2017/05/ftc-settlement-amazon-yields-70-million-consumers-advice> (2017 Amazon settlement); Cecilia Kang & David McCabe, *F.T.C. Broadens Review of Tech Giants, Homing in on Their Deals*, N.Y. TIMES (Feb. 11, 2020), <https://www.nytimes.com/2020/02/11/technology/ftc-tech-giants-acquisitions.html> (2020 Amazon, Apple, Facebook, Alphabet, and Microsoft investigation); Microsoft Corp., FED. TRADE COMM'N, <https://www.ftc.gov/enforcement/cases-proceedings/002-3331/microsoft-corporation> (last updated May 18, 2001) (2001 Microsoft settlement); Spencer Soper & Ben Brody, *Amazon Probed by U.S. Antitrust Officials over Marketplace*, BLOOMBERG (July 24, 2019, 5:00 AM), <https://www.bloomberg.com/news/articles/2019-09-11/amazon-antitrust-probe-ftc-investigators-interview-merchants> (2019 Amazon-specific antitrust investigation); Nick Statt, *Facebook Confirms New FTC Antitrust Investigation After Posting Strong Earnings*, THE VERGE (July 24, 2019, 4:27 PM), <https://www.theverge.com/2019/7/24/20726371/facebook-ftc-antitrust-earnings-q2-2019-privacy-regulation-mark-zuckerberg> (2019 Facebook-specific antitrust investigation).

¹⁴⁷ Between the enormous range of sectors Amazon is involved in through its provision of cloud services and the range of sectors that sell products through its site, and the fact that on-line advertising is overwhelmingly dominated by Facebook and Google, all kinds of competition and consumer protection investigations will necessarily involve these companies. See, e.g., Khan, *supra* note 61, at 768–78 (describing how Amazon leverages its delivery infrastructure into outpricing competitors in a range of industries, such as when it eliminated its biggest competitor in diapers and other baby care goods through a carefully orchestrated predatory pricing scheme and ultimate acquisition). Amazon accounted for over a third of online retail sales in the United States last year. Jessica Young, *US Ecommerce Sales Grow 14.9 percent in 2019*, DIGITAL COM. 360 (Feb. 19, 2020), <https://www.digitalcommerce360.com/article/us-ecommerce-sales/>. The FTC is also currently undergoing a review of Amazon, Apple, Facebook, Alphabet, and Microsoft's reliance on "killer acquisitions"—i.e., the practice of buying a nascent competitor to neutralize the threat posed by the smaller company's product. Kang & McCabe, *supra* note 146.

¹⁴⁸ Memorandum from the Comm. on Energy & Commerce Staff, *supra* note 75.

technologists on staff has been a frequent point of criticism by advocates,¹⁴⁹ former¹⁵⁰ and current¹⁵¹ FTC officials, and Congress,¹⁵² and the agency has acknowledged the deleterious effects of the lack of technologists on its effectiveness.¹⁵³ The overly broad application of the conflict rules exacerbates this problem.

V. POLICY RECOMMENDATIONS

We offer policy recommendations to address this problem and help pave the way for the FTC and other Federal agencies to increase their technical capacity. The FTC has joined Congress and civil society in bemoaning its lack of technical experts, and it must mitigate the obstacles that currently make correcting this problem so difficult. We offer specific suggestions and broader objectives that will help mitigate the current obstacles the agency faces in order to attract and retain technology expertise.

To be clear, we do not mean to diminish the need for conflict of interest laws, nor do we support watering down the efficacy of those laws to prevent corruption or slow the revolving door. We see civil service as an important, if not sacred, calling, and we endorse the strong use of conflicts rules to discourage cynical or opportunistic people from trading on government service for personal gain. In fact, we think in some cases conflict of interest laws may need to be strengthened as there are still a great deal of former employees that “switch sides” and join companies the agency is tasked to oversee.¹⁵⁴

However, we believe that the FTC-administered rules go far beyond these important goals, especially when applied to technologists.¹⁵⁵ As discussed above, in many cases, former FTC technologists seek simply to work on the same side as the agency in the furtherance of consumer protection.¹⁵⁶ In those situations, we think a re-evaluation of priorities is warranted.

First, the FTC should address the current vagueness in determining when different projects comprise either the same “proceeding or investigation” under 16 C.F.R. § 4.1(b) or the same “particular matter” under 18 U.S.C. § 207(a). Under the current formulation of the rule, in making this determination the FTC considers “the extent to which the matters involve the same or related facts, issues, confidential information and parties; the time elapsed; and the continuing existence of an important Federal interest.”¹⁵⁷ The FTC could interpret this broad set of factors as

¹⁴⁹BECKY CHAO, ERIC NULL & CLAIRE PARK, OPEN TECH. INST., ENFORCING A NEW PRIVACY LAW: WHO SHOULD COMPANIES HOLD ACCOUNTABLE? (2019), <https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/> (noting the paucity of technologists at the agency and noting that it is “unclear whether the FTC has the technological expertise it needs to enforce privacy laws”).

¹⁵⁰McSweeney, *supra* note 50, at 530 (recommending that the FTC “scale[] up its in-house technology and research expertise”); Jessica Rich, *Give the FTC Some Teeth to Guard Our Privacy*, N.Y. TIMES (Aug. 12, 2019), <https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html> (“To adequately police privacy in this country, the F.T.C. needs more lawyers, more investigators, more technologists and state-of-the-art tech tools. Otherwise, it will continue to operate on a shoestring, foregoing certain investigations and understaffing others.”).

¹⁵¹See, e.g., OFFICE OF COMM’R ROHIT CHOPRA, FED. TRADE COMM’N, COMM’N FILE NO. P065404, STATEMENT OF COMMISSIONER ROHIT CHOPRA: REGARDING THE REPORT TO CONGRESS ON THE FTC’S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY 4–5 (2020), https://www.ftc.gov/system/files/documents/public_statements/1577067/p065404dpp_choprastatement.pdf.

¹⁵²See, e.g., Memorandum from the Comm. on Energy & Commerce Staff, *supra* note 75; Hearing on “Oversight of the Federal Trade Commission: Strengthening Protections for Americans’ Privacy and Data Security” Before the Subcommittee on Consumer Protection and Commerce of the House Committee on Energy and Commerce, 116th Cong. (2019) (opening statement of Rep. Jan Schakowsky, Chair), <https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/2019.5.8.SCHAKOWSKY.%20FTC%20Oversight%20Hearing.CPC-0.pdf> (noting a contributing factor to the agency’s struggle to conduct meaningful enforcement is the mere five technologists and lack of a Chief Technologist).

¹⁵³*The Technology 202: The Government’s Top Silicon Valley Watchdog Only Has Five Full-Time Technologists. Now It’s Asking Congress for More*, WASH. POST (Apr. 4, 2019, 8:47 AM), <https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/04/04/the-technology-202-the-government-s-top-silicon-valley-watchdog-only-has-five-full-time-technologists-now-it-s-asking-congress-for-more/5ca512661b326b07f38f30d/> (discussing a letter from FTC Chairman Joseph Simons to the House Committee on Energy and Commerce “request[ing] funding for 10 to 15 more technologists”).

¹⁵⁴Janofsky & Drange, *supra* note 143.

¹⁵⁵See discussion in *supra* Section III.A.

¹⁵⁶*Id.*

¹⁵⁷16 C.F.R. § 4.1(b)(1) n.1. In setting forth these factors, the FTC refers to an analogous section of the Office of Government Ethics’ regulations setting forth the factors considered to determine whether two particular matters are the same under § 207: “the extent to which the matters

permitting it the latitude to determine that “same side” investigations that take place after an FTC settlement complaint has already been brought constitute new and separate “proceeding[s] or investigation[s].” At present, however, the FTC interprets the vagueness of this multi-factor test to apply post-employment restrictions extremely broadly, in a way that we believe ultimately runs counter to the public interest.

Second, the FTC should clarify that whether or not one particular “proceeding or investigation” is the same turns more narrowly on the specific facts of the underlying investigation. The 2012 consent decree with Facebook speaks to this.¹⁵⁸ The consent decree stemmed from an investigation into, among other things, changes to Facebook’s privacy policies that made more information about its users visible to the public than before and misled consumers about the amount of information third-party apps could obtain about users.¹⁵⁹ The investigation led to a settlement and twenty-year consent decree that obligated Facebook to create a “comprehensive privacy program” and to report to the FTC for twenty years.¹⁶⁰

For former FTC officials who worked on the 2012 consent decree, what is the underlying matter that might trigger conflicts review today? We contend that the matter should be closely related to the facts that existed in 2012, which was largely premised on changes to privacy policies in 2009 and 2010 as well as aspects of Facebook’s architecture in 2011. In contrast, the FTC seems to take a much broader interpretation, treating the underlying “matter” as “Facebook and privacy.” For example, the FTC has prevented at least one of us from working on cases related to Cambridge Analytica, the company that notoriously mined Facebook user data in the 2016 election, by claiming they were too closely related to the 2012 consent decree matter, even though Cambridge Analytica did not even exist in 2011.¹⁶¹ The FTC allowed another of us to participate in a matter related to Cambridge Analytica but only after a two-week delay that prevented a more meaningful role in the case. A definition of “proceeding or investigation” as expansive as “Facebook and privacy” or “Amazon and predatory pricing” will disqualify the FTC’s technologists from working on crucial investigations, even as these companies consistently repeat the same kind of exploitative practices and necessary technological expertise becomes harder and harder for enforcers to find, attract, and retain.

Third, to bring even more clarity to its conflicts analysis, the FTC should consider announcing a bright-line rule in the form of a time limit on conduct that will be considered the same “matter” or “proceeding or investigation.” For example, the FTC might decide that, for investigations into the conduct of platforms, such as social networking services or search engines, it is not the same “matter” if it occurs more than two years after an earlier matter, nor is an investigation the same “proceeding or investigation” if it arises more than two years later. This approach finds support in the rhetoric of the FTC itself, which regularly publishes paeans to the speed and dynamism of innovation in the technology industry.¹⁶²

involve the same basic facts, related issues, the same or related parties, time elapsed, the same confidential information, and the continuing existence of an important Federal interest.” 5 C.F.R. § 2641.201(h)(5)(i).

¹⁵⁸ Decision and Order, 5–8, In the Matter of Facebook, Inc., Fed. Trade Comm’n (Aug. 10, 2012) (Docket No. C–4365), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>

¹⁵⁹ Press Release, Fed. Trade Comm’n, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

¹⁶⁰ Decision and Order at 5–8, Facebook, Inc., No. C–4365 (Fed. Trade Comm’n Aug. 10, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>; Press Release, Fed. Trade Comm’n, FTC Approves Final Settlement with Facebook (Aug. 10, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>.

¹⁶¹ Cambridge Analytica was founded in 2013. See David Ingram, *Factbox: Who Is Cambridge Analytica and What Did It Do?*, REUTERS (Mar. 19, 2018, 10:00 PM), <https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F>.

¹⁶² See, e.g., Request for Public Comment on the Federal Trade Commission’s Implementation of the Children’s Online Privacy Protection Rule, 84 FED. REG. 35,842, 35,843 (July 25, 2019); FED. TRADE COMM’N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? i (2016) (“With a smartphone now in nearly every pocket, a computer in nearly every household, and an ever-increasing number of Internet-connected devices in the marketplace, the amount of consumer data flowing throughout the economy continues to increase rapidly.”); STAFF OF THE FED. TRADE COMM’N, PROTECTING CONSUMERS IN THE NEXT TECH-ADE 2 (2008) (“Consumers’ roles are changing in this new marketplace, as are the products they buy, how those products are marketed and advertised, and how they are paid for . . . [and] at a dizzying pace.”); Maureen K. Ohlhausen, *The Procrustean Problem with Prescriptive Regulation*, 23 COMMLAW CONSPECTUS 1, 2 (2014) (“When the regulated industry is rapidly evolving, yesterday’s comfortable regulatory bed can quickly become a torture rack for tomorrow’s technologies.”); Maureen K. Ohlhausen,

To blunt the potential arbitrariness of a rigid two-year deadline, this gloss on the FTC rules can be presented as a rebuttable presumption: facts will be presumed not to involve the same matter after two years, but the FTC can rebut the presumption by marshaling specific facts demonstrating the same matter.

Fourth, the FTC should also revise its rules to make it easier for former technologists to consult on “same side” investigations, such as those conducted by state attorneys general. To do this, the FTC should revise its definition of “communicate to or appear before”—a key definition that serves to specify which types of activities by former employees are subject to restriction.¹⁶³ Under the current definition, the FTC’s rules are triggered when a former employee engages in “any oral communication or written communication to, or any formal or informal appearance before, the Commission or any of its members or employees on behalf of any person (except the United States) with the intent to influence.”¹⁶⁴ We recommend that the agency add “or the Government of one of the States” to the parenthetical exception. The purpose of the rules is to enable more effective enforcement of the law by preventing agency capture or the appearance of corruption, and the exception acknowledges that other work on behalf of the government does not present that concern. The exception easily could—and should—be extended to work on behalf of state attorneys general, which support the agency’s consumer protection and competition mission.

The FTC’s rules must be revised, but in the meantime, the OGC can also simply exercise its discretion to grant more clearance requests from former technologists seeking to work on investigations on behalf of state attorneys general. In laying out prohibited conduct for former employees, the text of the rules clarifies that post-employment conduct may be “otherwise specifically authorized by the Commission,” though the rules do not elaborate further about what those circumstances might be.¹⁶⁵ In addition, § 207 includes a specific exception for former employees that provide scientific or technological information. That exception states in part that certain § 207 restrictions do not apply “with respect to the making of communications solely for the purpose of furnishing scientific or technological information, if such communications are made under procedures acceptable to the department or agency concerned.”¹⁶⁶ In many instances, state attorneys general seek former technologists’ advice on policy and strategy, not solely for scientific or technological information. However, there are circumstances in which the FTC could rely on this exception to quickly bless requests from former technologists to provide scientific or technological information to other parties, particularly those on the “same side.” Yet FTC staff never even mentioned the existence of this exception to those of us who are former technologists when we sought advice on possible conflicts.

In addition, the FTC should create greater transparency into its substantive evaluation of clearance requests, as well as into the procedures it applies in considering those requests. At present, it is difficult for members of the public and, indeed, former technologists themselves to gain insight into this process. Under the FTC’s rules, “[a]ny request for clearance filed by a former member or employee pursuant to this section, as well as any written response, are part of the public records of the Commission, except for information exempt from disclosure under § 4.10(a) of [the] chapter.”¹⁶⁷ However, documents related to clearance requests are not available on the FTC’s website or in its “FOIA Reading Room.” We submitted a request to the FTC under the Freedom of Information Act for “[a]ll documents relating to

Acting Chairman, Fed. Trade Comm’n, Antitrust Enforcement in the Digital Age, Remarks Before the Global Antitrust Enforcement Symposium 6, 11 (Sept. 12, 2017) (describing technology markets as “fast-moving”); Neil Brady, *‘Velocity’ of Technological Change ‘Speeding Up’ Says FTC Commissioner*, MEDIUM (July 11, 2017), <https://medium.com/@neil.brady/speed-of-technological-change-increasing-sense-of-loss-of-control-says-ftc-commissioner-259265f4389f> (accounting how the former FTC Commissioner Terrell McSweeney noted that the “velocity of technological change is speeding up”); Lesley Fair, *Future of the COPPA Rule: What’s on the Agenda*, FED. TRADE COMM’N: BUS. BLOG (Oct. 1, 2019, 11:46 AM), <https://ftc.gov/news-events/blogs/business-blog/2019/10/future-coppa-rule-whats-agenda> (“Technology changes at the speed of light, but the touchstone of the Children’s Online Privacy Protection Rule remains constant.”); *Financial Technology: Protecting Consumers on the Cutting Edge of Financial Transaction*, FED. TRADE COMM’N, <https://www.ftc.gov/news-events/media-resources/consumer-finance/financial-technology> (last visited Aug. 23, 2020) (describing the agency’s approach to the “fast-moving realm of financial technology”).

¹⁶³ See 16 C.F.R. § 4.1(b)(1) (restricting when a “former member or employee . . . of the Commission may communicate to or appear before the Commission, as attorney or counsel, or otherwise assist or advise behind-the-scenes, regarding a formal or informal proceeding or investigation”).

¹⁶⁴ 16 C.F.R. § 4.1(b)(5)(ii).

¹⁶⁵ 16 C.F.R. § 4.1(b)(1).

¹⁶⁶ 18 U.S.C. § 207(j)(5).

¹⁶⁷ 16 C.F.R. § 4.1(c).

clearance requests filed by former FTC employees under 16 C.F.R. § 4.1(b)(2)” from January 2017 to March 2020, but our request was denied on the basis that “the resources required to process your request would cause an unreasonably burdensome review process for the agency.”¹⁶⁸

The agency’s clearance process should also be clarified so that ex-employees know what to expect. The FTC’s rules set forth particular procedures for FTC consideration of clearance requests filed by former employees. But in our experience, the staff of OGC frequently dismiss clearance requests informally over e-mail, without either directing former employees to file formal requests pursuant to the FTC’s rules or referring the matter to the Commission for approval.¹⁶⁹

We also propose that OGE revise its regulations under § 207. In particular, OGE should vest Federal agencies, including the FTC, with clearer authority to determine when a particular “matter” is the same as another for purposes of applying § 207. At least where independent agencies are concerned, we propose that this interpretative authority lie with the specific agency where a former Federal employee previously served. This would constitute a modest shift from OGE’s current guidance that the agency where an employee previously served may advise the employee as to the application of § 207 but that any advice it provides will not be binding on the DOJ.¹⁷⁰ Granting clearer deference to Federal agencies—including the FTC—on the question of whether or not two particular matters are the same may empower the FTC to make the determination based on whether or not it believes there is a true conflict of interest, rather than based on the agency’s over-prudent estimation of the broadest way in which the DOJ could possibly construe the question itself.

Finally, parallel reforms would also help alleviate the problems we have outlined, or at least they would help ensure that even if former technologists continue to be broadly precluded from contributing to similar work with other agencies, this disincentive does not completely halt the influx of technologists interested in public service. For example, a modest raise to the pay scale for government employees would help attract technologists. It is a tall order to expect recently graduated computer scientists to turn down six-figure salaries working for technology companies in the background of financial burdens like substantial student debt or supporting families.¹⁷¹ Students with fewer resources are disproportionately deterred from government service, which results in a Federal service that is disproportionately wealthier than the rest of the population. Public service should not be a vocation reserved for the independently wealthy. The practices of technology companies implicate every part of society, and we need enforcers with diverse backgrounds and prior experiences. Moreover, paying public servants at rates more comparable with the private sector would help to reduce the revolving door problem. Agency employees, congressional aides, and public servants at all levels of government would not need to leave the government out of financial necessity if government service paid comparable rates to the private sector. Public service may be a calling, but a calling cannot feed children or pay a landlord.

VI. CONCLUSION

Few question the dire need for technological expertise at the U.S. consumer protection and competition agency. Yet, the FTC is exacerbating its existing difficulty in recruiting and retaining technologists by unduly limiting the kind of work technologists can undertake after leaving government service. The FTC’s interpretation and uneven application of well-intentioned conflict rules further undermine not only its own efficacy, but also the efficacy of complementary enforcement bodies that support the agency’s mission. We urge a series of modest reforms to prevent post-employment restrictions from hamstringing the FTC’s enforcement efforts as well as those of other agencies. We hope these reforms will also help pave the way for

¹⁶⁸ Freedom of Information Act (FOIA) request and response on file with authors.

¹⁶⁹ See 16 C.F.R. §§ 4.1(b)(6)–(7).

¹⁷⁰ 5 C.F.R. §§ 2641.105(a), (c). This would also be consistent with at least one Federal appellate case that considered a “same particular matter” question in an instance where the agency in question had advised the former employee that two matters were not the same. *CACI, Inc. v. United States*, 719 F.2d 1567, 1576 (Fed. Cir. 1983) (“This ruling is entitled to weight. It would be most unusual to disqualify [former employee] Sterling from bidding on the proposal because of Stevens’ participation for Sterling after the Assistant Attorney General in charge of the Antitrust Division had advised Sterling that Stevens’ handling of the proposal for Sterling would not be improper.”).

¹⁷¹ See Adam Janofsky & Matt Drange, *We Counted the FTC Employees who Moved Over to Tech. Is Reform Needed?*, PROTOCOL (Mar. 9, 2020), <https://www.protocol.com/ftc-tech-hawley-revolving-door/> (quoting one former FTC employee who now works for Electronic Arts as saying that it can be “very difficult to live there on a government salary, especially if you have student loan debt”).

skilled technologists to seek and secure meaningful careers in public service without unnecessarily hemming in their future career prospects.

The CHAIRWOMAN. Thank you. Thank you very much. We will now hear from Mr. Morgan Reed from The App Association who is here in person. Thank you.

**STATEMENT OF MORGAN REED, PRESIDENT,
ACT | THE APP ASSOCIATION**

Mr. REED. Chairman Cantwell, Ranking Member Wicker, my name is Morgan Reed and I am the President of ACT | The App Association. We are a leading trade group representing small software and device companies in the app economy, a \$1.7 trillion global sector that supports roughly 5.9 million jobs here in the U.S.

I am here to share the perspectives of App Association members, many of which are in your states, on the need for strong Federal privacy laws and enforcement. And when I say in your state, I am not doing some kind of hand waving blanket gesture, I am talking about real companies. Chair Cantwell, in Spokane we have Mighty Call, which provides a cloud based communications platform for small businesses to connect teams remotely. In Starkville, we have got Buzzbassador. They provide a management platform for brands to use Ambassadors promoting a product across social media.

And in my written testimony, there are examples for every single one of your states and in every single one of the districts in this country. We changed the way we are doing business today, whether it is farming, education, communication, and sometimes just having fun. These companies rely on consumer trust much more than large companies with brand recognition and privacy is the leading factor.

According to Pew, 63 percent of consumers say they have deleted an app due to privacy concerns, and 65 percent cite trust in brand as their number one consideration when deciding whether to allow access to their information. My member companies are small and can't buy a Super Bowl ad to create brand awareness. So when we try to reach customers through the app stores, we rely heavily on the trustworthiness of the ecosystem and the marketplaces within. The Federal Trade Commission and this committee play an important role in maintaining that trust by maximizing consumer protection while fostering growth in the economy.

To better protect consumer privacy, we urge you to take these four considerations into account. Number one, Congress should set the scope and purposes of the FTC enforcement authority and resources on privacy. The existing regulatory framework for the FTC does not have the tools to deal with the more complex data and privacy questions that arise. The rest of the world has surged ahead of the U.S. on these questions. When Europe instituted the GDPR, it was clear the U.S. would have to act, if just to harmonize.

But now 16 other countries have national privacy laws matching GDPR, and as Chair—as Ranking Member Wicker noted, there are 100 more countries with some form of national privacy law, and the U.S. still has nothing. The FTC needs better privacy tools based on the risks data processing activities posed to consumers and the expectations that people have about its use. It is up to Congress to set forth the overarching purposes and specify the limits on FTC rules.

Failure to act hurts American citizens and American competitiveness globally. Number two, if Congress doesn't act, we have seen what—how FTC is forced to stretch their authority. The FTC's recent effort to use breach notification to cover unauthorized sharing is an example how the FTC has to cobble together a solution in the absence of Congressional action. Just like Tom Hanks character in the movie *Cast Away* using ice skates to open coconuts, the Commission is settling for the tools it can find rather than the right tool when it proposes to enforce a breach notification rule as a privacy law. But we are not on a desert island.

Congress can and should make the right tools for the job. Number three, Congress should produce more—should produce one national privacy framework. The single most important policy decision Congress can make to combat existing and future privacy harms is to enact comprehensive privacy legislation that grants strong consumer rights to the citizens of all 50 states simultaneously. A patchwork will make it hard for small businesses like mine and comparatively easy for big companies with hundred lawyer compliance departments. In short, preemption is essential to the success for the little company. And number four, Congress should avoid antitrust measures that prohibit some of the most important platform level privacy controls consumers and app makers rely on today. Big companies doing business on the app stores, Epic games and Spotify and others, have their own big brand, and some of them don't want the app stores to manage the platform.

However, we urge you not to undermine trust in the app economy with bills that would prevent key privacy protections my members rely on to bring consumers to market. To be clear, we are not opposed to and in fact support the FTC vigorously enforcing the law on privacy and on unfair methods of competition. For example, on the competition side, the Commission has the opportunity to clarify the applicability of its UMC authority to standards essential patents.

Anti-competitive self-abuse harms consumers and small businesses and competition alike, and this is an example of where the FTC guidance can help. But ultimately, the economic, health, education and frankly, opportunities for growing new businesses created for—in our country, depend on a robust and appropriately funded FTC.

Congress needs to get this right and they need to do it now. And without it, we are left with giving the FTC a pile of money and they are going to end up spending it on additional ice skates to open coconuts rather than the tools that they need to solve the problems that we face today. Thank you.

[The prepared statement of Mr. Reed follows:]

PREPARED STATEMENT OF MORGAN REED, PRESIDENT, ACT | THE APP ASSOCIATION

Executive Summary

ACT | The App Association (the App Association) is the leading trade group representing small mobile software and connected device companies in the app economy, a \$1.7 trillion ecosystem employing 186,590 people in Washington and 14,190 in Mississippi.¹ Our member companies create the software that brings your smart

¹ACT | THE APP ASSOCIATION, STATE OF THE U.S. APP ECONOMY: 2020 (7th Ed.), available at <https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf>.

devices to life. They also make the connected devices that are revolutionizing healthcare, education, public safety, and virtually all industry verticals. They propel the data-driven evolution of these industries and compete with each other and larger firms in a variety of ways, including on privacy and security protections.

One of the foundational imperatives for the success of small business innovators in the app economy is consumer trust in the marketplace. The vast majority of mobile device users cite trust as the number one factor when deciding to grant an app access to their personal data, and users already commonly restrict access and delete apps they believe pose a privacy risk.² Eighty-nine percent of users have at some point denied features, such as microphone or location access, to an app they did not trust, while 63 percent of users have deleted an app outright due to privacy concerns.³ Because our member companies are small and often young companies, they rely more heavily on the privacy and security protections and controls that protect consumers from bad actors than their larger, more established counterparts—which depend more on brand name reputation and recognition. Therefore, the Committee's and the Federal Trade Commission's (FTC's) role in holding bad actors accountable is critical to the success of App Association members. Specifically, we urge you to take the following recommendations into account as you evaluate next steps on consumer privacy:

1. *Congress Should Guide FTC Enforcement Authority and Resources.* Though the FTC is the main privacy enforcer at the Federal level and has its hands full in recent years with the proliferation of privacy, security, and other consumer protection issues, it often lacks the statutory authority and/or dedicated funding to carry out its mission to the fullest potential.
2. *Congress Should Avoid Forcing the FTC to Stretch its Own Authority.* The FTC's recent steps to bolster its leadership in the privacy space, while certainly understandable, demonstrate that the Commission is working with limited tools at its disposal.
3. *Congress Should Enact a Federal Privacy Framework.* The single most impactful policy decision Congress can make to combat existing and future privacy harms is to enact comprehensive privacy legislation that grants strong consumer rights to the citizens of all 50 states simultaneously.
4. *Congress Should Avoid Antitrust Measures that Presume the Illegality of Platform-Level Privacy Protections.* These proposals could unintentionally render widely-adopted privacy protections illegal, especially those that consumers use on their smart devices, exposing consumer data to greater privacy and security risks.

We deeply appreciate your leadership as the Senate Commerce Committee continues to navigate the unprecedented COVID-19 pandemic and works to get our economy back on track. As part of these efforts, we ask that you continue the bipartisan work of crafting a single set of rules governing the privacy practices of entities that generally fall under the FTC's jurisdiction. Recent events and the forced shift of daily and essential activities—including core healthcare and communication services—to the digital space has underscored the need for Congress to act decisively on this issue.

I. Congress Should Guide FTC Enforcement Authority and Resources

We support enhancing the enforcement capabilities and resources for the FTC to stop and prevent consumer protection harms by bad actors. The FTC needs more appropriate tools with Congress' direction to stop consumer harms resulting from privacy and data security abuses in particular, as those problems have proliferated and continue to generate headlines and stoke constituent outrage.

Recent activity in the House Energy & Commerce Committee indicates that lawmakers are seriously mulling increased funding for the FTC as part of ongoing deliberations on the budget reconciliation package. In particular, the House Energy & Commerce Committee voted to approve \$1 billion in additional appropriations for the Commission to establish new a privacy bureau to conduct work "related to unfair or deceptive acts or practices relating to privacy, data security, identity theft,

² 14. DELOITTE, TRUST: IS THERE AN APP FOR THAT? DELOITTE AUSTRALIAN PRIVACY INDEX 2019, (2019), available at <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-150519.pdf>.

³ *Id.* at 6

data abuses, and related matters.”⁴ In general, App Association members support vigorous management of the marketplace for bad actors, especially those that circumvent rules in a way that reduces overall trust in the app ecosystem or that threaten an even playing field in the marketplace. However, in this case, we believe that Congress should not act in half measures on privacy and that empowering the FTC with augmented capabilities to address privacy harms should take the form of a comprehensive Federal privacy regime. Simply establishing a new bureau with additional resources does little to enhance enforcement remedies, nor does it more clearly delineate the breadth and boundaries of the FTC’s authority on privacy practices.

We also appreciate and understand the intent behind proposals originating in the House Energy & Commerce Committee to bolster the FTC’s enforcement authority. At the same time, we continue to have concerns with granting the Commission, or any new regulatory body, general, *undirected* rulemaking authority to regulate privacy harms. The same concerns extend to even more general rulemaking authority to regulate *all* consumer protection harms under the FTC’s purview. As we’ve previously written, we recommend providing only narrow rulemaking authority on the issue of privacy, as “[t]he swath of the economy and range of economic activities” any privacy regulator would oversee is “too broad for it to promulgate generally applicable rules that successfully balance the finer conflicts of purpose in the many sectors that would be subject to those requirements.”⁵ A general grant of rulemaking authority to define unfair or deceptive acts or practices in or affecting commerce would completely delegate the exercise of defining limits to the Commission’s own powers to the agency itself—a task better suited to Congress. A Democratic Congress imposed additional procedural hurdles on the Commission’s rulemaking authority in 1980⁶ for just this reason. The sheer breadth of its purview was better adapted for an adjudicative approach and invited overreach with rulemaking.

Aside from potential overreach and its relative unsuitability in regulating the dynamic markets the FTC oversees, general rulemaking also creates substantial uncertainty and potential instability. For example, an FTC controlled by one party might construct a carefully segmented regulatory regime, categorizing consumer protection harms by industry. The next Administration might have a completely different regulatory philosophy and scrap the framework entirely. Without guardrails in statute, challenges to such a complete deletion of regulations might fail—according to jurisprudence evaluating Federal agency decision-making, the courts grant “*Chevron* deference” to those interpretations.⁷ The less there is for an agency to interpret, the more leeway an agency has to define its own goals and decisions.⁸ The result could be massive swings in consumer protection regulation from one agency to the next (mainly unchecked by the courts), and in all likelihood, a more purposeful focus on political aims and headlines rather than targeting practices that are net harmful to consumers. Even where Congress has explicitly outlined regulatory goals and purposes, shifts in Administration have brought uncertainty, especially to more dynamic markets. The effect could be much worse without clear statutory guidance on the limits and purposes of FTC rules and enforcement.

As Rob Coons, chief revenue officer of App Association member Walker Tracker—a platform for people to compete with each other on step challenges and similar wellness activities—points out, regulatory uncertainty falls heavily on small companies like his. For example, as states and governments overseas recently enacted new and differing general consumer privacy laws, Walker Tracker went back to the drawing board on its data processing agreements with employer clients. In turn, Walker Tracker now turns down contracts under a certain dollar threshold with smaller companies because the costs of uncertainty are too high to justify working on smaller contracts. Further privacy shifts at the state level coupled with regulatory pirouetting at the Federal level would only worsen the situation for Walker Tracker and other App Association members.

We have similar concerns with granting the Commission broad civil penalty authority for any violation of the FTC Act, as legislation pending in the House would do. Although we support granting the Commission civil penalty authority for specific

⁴ See Committee Print by the Committee on Energy and Commerce, Title III, Subtitle O, § 31501, available at <https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2021/09/BILLS-117pih-SubtitleO.pdf>.

⁵ Letter from Graham Dufault and Madeline Zick to the Honorable Anna Eshoo and the Honorable Zoe Lofgren, Members of Congress, re: Draft Framework of Online Privacy Act of 2019 (Jul. 18, 2019).

⁶ See the Federal Trade Commission Improvements Act of 1980 (H.R. 2313, 96th Cong.).

⁷ See *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984); *Astrue v. Capato*, 566 U.S. 541 (2012).

⁸ *Id.*

kinds of offenses, including as part of a general privacy bill, civil penalties for cases of first impression would chill innovation that has a net positive effect on consumer welfare. For example, when the Commission first encountered social media influencers, it quickly developed guidance outlining proper disclosures for influencers who receive compensation for endorsing products and services.⁹ A fast-developing business that blurred the lines between personal networking and advertising, “influencing” cried out for FTC clarity on when it crosses the line into deception. If the FTC had civil penalty authority—providing up to \$44,000 per violation—in cases where market participants have little notice as to where the line is for social media influencing, the cost of those potential penalties might have discouraged the practice altogether. Although influencing may have gained an unserious reputation,¹⁰ its emergence created legitimate livelihoods where none previously existed. And while authorizing civil penalties for first offenses—under the broad prohibitions in Section 5—would not necessarily cause the FTC to shoot first and ask questions later, it certainly could allow for such an enforcement approach.

The risk of such a regime falls especially heavily on small companies like App Association members. Marc Fischer, chief executive officer of App Association member Dogtown Media, says the prospect of civil penalties in undefined cases could cause longer timelines for product and service development and higher insurance costs. Dogtown Media is a mobile media development firm that has created more than 200 apps on behalf of clients in a wide variety of industries, and like many of its peers, buys business risk insurance. As Marc points out, those costs would likely increase with the prospect of monetary penalties for first-time offenses, and the additional money he spends on those premiums should instead go toward hiring and business development.

The concerns are especially acute where companies, like Dogtown Media, are forging cutting edge uses for advanced technologies like artificial intelligence (AI). Publicly traded firms with high-powered attorneys may be able to pay heavy fines and move on, but those penalties could deal a devastating financial blow to small companies like App Association members.

Other reform proposals on the House side that would enhance the FTC’s authority cause similar concerns for our member companies, although we would support these limited expansions in some forms in the context of a general privacy bill. For example, possible reforms could expand the FTC’s jurisdiction to cover non-profit entities or expand FTC jurisdiction to cover common carriers under the Communications Act (telecommunications and wireless carriers, for example). It may make sense to enable the FTC to cover these kinds of entities in a more limited context like a general privacy bill, but we would be concerned about adding breadth to the FTC’s purview generally. For Communications Act common carriers and non-profit entities, we have seen provisions in privacy bills that would place both categories into FTC jurisdiction—while carving those common carriers out of Communications Act jurisdiction—for the purposes of the privacy law and regulations promulgated under it.¹¹ The FTC is a more experienced privacy enforcer than the Federal Communications Commission (FCC), so it makes sense to task the FTC with monitoring privacy practices of wireless carriers instead of the FCC. The targeted treatment of telecommunications common carriers also avoids overlapping regulation of certain entities by multiple Federal agencies. App Association members demand high quality services at the lowest possible costs from Internet service providers and understand that subjecting them to duplicative regulatory compliance and penalties from multiple Federal agencies could increase costs and diminish service quality.

II. Congress Should Avoid Forcing the FTC to Stretch Its Own Authority

Absent action from Congress to grant additional rulemaking authorities to the Commission, either through a comprehensive privacy law or otherwise, the Commission is likely to take it upon itself to reinterpret its existing authorities to better police the marketplace. While certainly an understandable impulse in the face of a rapidly evolving digital ecosystem and host of novel privacy harms, this direction also predictably produces suboptimal outcomes for businesses and consumers.

The recent policy statement issued by the FTC interpreting its Health Breach Notification Rule is emblematic of the limitations and issues that can arise when the Commission stretches its limited powers beyond their intended purpose. During its

⁹ DISCLOSURES 101 FOR SOCIAL MEDIA INFLUENCERS, FED. TRADE COMM’N (Nov. 2019), available at https://www.ftc.gov/system/files/documents/plain-language/1001a-influencer-guide-508_1.pdf.

¹⁰ Influencers in the Wild, @influencersinthewild, INSTAGRAM, <https://www.instagram.com/influencersinthewild/?hl=en> (last visited Jul. 25, 2021).

¹¹ See, e.g., SAFE DATA Act (S. 4626, 116th).

most recent open meeting, FTC Commissioners voted 3–2 to approve a policy statement affirming that health apps and connected devices that collect or use consumers’ health information must comply with the Health Breach Notification Rule. The FTC originally implemented its Health Breach Notification Rule in September 2009, as required as part of the American Recovery and Reinvestment Act of 2009, though it has yet to enforce the rule in its more than 10 years of existence. The rule requires that vendors of personal health records (PHRs) and their service providers notify consumers and the FTC when a breach of identifiable health information occurs. Failure to report such breaches carries civil penalties of up to \$43,792 per violation per day.

With its new policy statement, the Commission goes to great lengths to elide the difference between a breach of security and a privacy violation in hopes of expanding the rule’s reach. Whereas the Health Breach Notification Rule plainly states that it exists simply to ensure that PHR providers and their service providers notify consumers “when the *security* [emphasis added] of their individually identifiable health information has been breached,”¹² the policy statement asserts that whenever a health app *discloses* sensitive health information without users’ authorization, this is a “breach of security” under the rule.¹³ Notably, the Final Rule included several examples to elucidate what exactly a data breach means, all of which reference instances where information is taken or stolen *without* the provider’s knowledge.¹⁴ While we are sympathetic to the goal of preventing the unauthorized sharing of users’ sensitive information and agree that there should be punishment when a company violates consumer trust, the fact remains a data breach notification law is an odd vessel to accomplish those goals.

The policy statement also stretches the definition of PHR, which is defined in the rule to mean “identifiable health information on an individual that can be drawn from *multiple sources* [emphasis added] and that is managed, shared, and controlled by or primarily for the individual.” The policy statement instead asserts that health apps are covered by the rule even when the health information they collect comes from a single source (such as an application programming interface) and the user themselves inputs non-health data, such as through a separate calendar app. This directly contradicts existing FTC business guidance on the very topic, which states that “[i]f consumers can simply input their own information on your site in a way that doesn’t interact with personal health records offered by a vendor—for example, if your site just allows consumers to input their weight each week to track their fitness goals—you’re not a PHR-related entity.”¹⁵

The Health Breach Notification Rule is simply a poor fit for policing first-party privacy violations, and the FTC’s new interpretation could create numerous unintended consequences along the way. For example, since the notification standard in the rule is triggered when the entity discovers the breach, FTC’s interpretation seemingly blesses the underlying unauthorized sharing of data so long as the provider proffers a notification after the fact. Or, instead, should the provider notify consumers when it first discovers its own plan to share the information with third parties? That either answer to the policy statement’s unanswered question generates a non-sensical outcome speaks to the frailty of the Commission’s interpretation.

To be fair, the Commission is genuinely seeking to address a rather worrisome gap in our Nation’s current privacy framework. And as Commissioner Rebecca Kelly Slaughter indicated, she looks forward to the Commission “taking more action to limit the unfair collection and use of data, especially through rulemaking.”¹⁶ Commissioners want to make the most of the authorities they have and we appreciate that they are focused on healthcare privacy in particular. The productive use of

¹² Health Breach Notification Rule, 74 Fed. Reg. 42962 (Aug. 25, 2009), available at https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf

¹³ Federal Trade Commission, Statement of the Commission On Breaches by Health Apps and Other Connected Devices (September 15, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

¹⁴ Health Breach Notification Rule, 74 Fed. Reg. 42966, § 318.2 (August 25, 2009), available at https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf

¹⁵ FTC Business Guidance, Complying with the FTC’s Health Breach Notification Rule, available at <https://www.ftc.gov/tipsadvice/business-center/guidance/complying-ftcs-health-breach-notification-rule>

¹⁶ Statement of Comm’r Rebecca Kelly Slaughter Regarding the Comm’n’s Policy Statement on Privacy Breaches by Connected Health Apps, Fed. Trade Comm’n, (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1596320/rks_remarks_on_health_breach_policy_statement_09152021.pdf.

healthcare data no longer only occurs with healthcare providers and other entities under the jurisdiction of the Health Insurance Portability and Accountability Act (HIPAA). The creation and flow of healthcare data outside the HIPAA umbrella has accelerated, even more so during the COVID-19 pandemic, and although the FTC has been active in enforcing its Section 5 authority, it does not possess first time enforcement authority to punish particularly egregious offenders.

These limitations were painfully illustrated in the recent settlement with Flo, a popular fertility and period tracking app that the FTC alleged shared the “health information of users with outside data analytics providers after promising that such information would be kept private.”¹⁷ Moreover, not only did Flo mislead consumers about its data sharing practices, but it also allowed third parties to use the data it shared for their own purposes.¹⁸ In some cases, this occurred in violation of the terms of service of those third parties, the data having been shared via software development kits (SDKs) they provided to Flo.¹⁹ These privacy missteps are especially concerning given the highly personal nature of the health information at issue.

Although Flo’s core deceptive statements in this case enabled the FTC to enjoin further harmful conduct, existing statute limited the Commission’s authority to wield monetary penalties to punish the company and signal to the marketplace that similar violations would not be tolerated. This is especially troublesome given that each and every headline detailing the deceptive conduct of firms using healthcare data outside the HIPAA umbrella threatens to further erode consumer trust, a key ingredient for success for our small business member companies. The healthcare innovations our member companies produce—from heart condition detection to chronic condition monitoring to simply managing digital health information across health systems—are far too important for us to let them fall victim to foundering consumer trust in digital health earned by bad actors.

From our perspective, the answer is not for the FTC to create novel or tenuous interpretations of its existing rules nor is it to extend HIPAA to cover healthcare tools and services not currently subject to HIPAA. As we’ve shown, the Commission will inevitably encounter roadblocks as it seeks to retrofit old rules to address new use cases. Meanwhile, HIPAA’s overarching purpose is to ensure the portability of health data between covered entities and business associates, and it was not primarily designed to give consumers better control over their own healthcare data or to manage the risks healthcare data processing poses.

III. Congress Should Enact a Federal Privacy Framework

In our opinion, the best way to improve FTC enforcement capabilities within the privacy sphere is to specifically grant those authorities as part of a Federal privacy framework.

We urge the Committee to establish a set of Federal requirements that puts in place baseline consumer rights and curbs data processing activities that expose consumers to undue privacy risks. For example, legislation introduced by the Committee chair and ranking member, as well as bipartisan draft legislation circulated by House Energy and Commerce Committee staff last year were a positive start representing substantial agreement on aspects of privacy that previously struggled for consensus. We urge you to continue the work on this effort and we stand ready to support negotiations and oversight activities around it.

Specifically, the App Association supports a Federal framework with the following attributes:

- *Transparency*
 - Federal privacy requirements should ensure businesses are transparent about the collection and use of information about consumers. App Association members compete on privacy and work hard every day to develop better ways to communicate with their users about privacy and give them meaningful choices. Consumers should have a clear understanding of the types of personal data they are sharing, and which companies are using that data and how.
- *Strong consumer rights*

¹⁷ Press release, “Developer of Popular Women’s Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data,” Fed. Trade Comm’n (Jan. 13, 2021), available at <https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc>.

¹⁸ Fed. Trade Comm’n, Flo Health, Inc., complaint (published Jan. 13, 2021), available at https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

¹⁹ *Id.*

- A Federal law should empower consumers to exert more control over their personal information, including the rights to access, correction, and deletion of such information. Sensitive personal information should also be subject to some limits on processing activities that pose too great a risk to consumers, which is not outweighed by countervailing benefits.
- *Accountability*
 - As the FTC has long argued, privacy should be built into the design and functionality of products and services. If privacy is a functional feature of a product or service, the protections, notices, and options it provides may shift and take on different forms depending on the context. Federal law should support the dynamic functionality of privacy by design by making companies accountable for sound privacy practices while allowing them to innovate on the details of their privacy programs.
- *A single, national standard*
 - New privacy legislation in Congress should establish a single, national standard and avoid creating a patent troll-style business model for trial attorneys to sue and settle with small companies through a broad private right of action. Our member companies may include the smallest software and connected device companies, but they each serve consumers across the Nation and around the world. Complying with a patchwork of state laws would be unnecessarily burdensome because their activities are not limited by any single state's borders. If privacy legislation does include a preemption provision, we would support limited rulemaking authority within statutory guidelines and limits for the FTC and allowing state attorneys general to enforce the bill's provisions.
- *Scalable requirements*
 - Federal privacy requirements should be scalable depending on the scope of an enterprise or data processing activities and the size and compliance capabilities of companies. App Association members do not want to be exempt from requirements—they want to comply with strong, flexible, and reasonable requirements.

Additionally, though several promising frameworks passed into law this year at the state level, including in Virginia and Colorado, we do not recommend that Congress wait around until the states cobble together a privacy patchwork that covers the Nation. Despite recent progress, at the current pace of passage, it would take decades for the individuals of all 50 states to gain coverage. Needless to say, Congress should not stand by idly as data abuses continue to proliferate in the states that opt against or are unable to pass a law.

Moreover, the more states that pass laws the greater the ambiguities and contradictions for businesses and consumers. Each of the three state privacy laws currently on the books include varying definitions for key terms, applicability thresholds, and sectoral exemptions. As more states enter the fray with their own laws, those nuances are only likely to multiply which makes compliance exponentially more difficult for businesses that operate across state lines (or have consumers in multiple states), while also increasing consumer confusion as to how their rights may or may not apply in a given scenario.

Finally, each new state law also improves the odds of a dormant Commerce Clause challenge, especially insofar as a new law directly contradicts another state privacy law or takes aim at a specific industry.²⁰ While this issue has yet to rear its head given the low number of state privacy proposals to make it from bill to law thus far, a constitutional challenge under the Commerce Clause could quickly stall the moderate progress at the state level bringing us back to square one. A preemptive Federal law is the only option that can avoid legal uncertainty, while effectuating uniform consumer rights across the Nation at the same time.

IV. Congress Should Avoid Antitrust Measures that Presume the Illegality of Platform -Level Privacy Protections

Software platforms (app stores together with mobile operating systems) play a key role in managing an app ecosystem that offers consumers a wide variety of options, while minimizing privacy risks. These management functions form the core of the

²⁰ Jennifer Huddleston and Ian Adams, "Potential Constitutional Conflicts in State and Local Data Privacy Regulations", Regulatory Transparency Project of the Federalist Society, (December 2, 2019), available at <https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf>

bundle of developer services App Association members purchase from platforms, without which consumer trust would be undermined. Some proposals in Congress, like the American Choice and Innovation Online Act (H.R. 3816) would presumptively prohibit these management functions, ostensibly to address complaints from competitors with alternative products and services on the platform. H.R. 3816 does this by prohibiting a software platform from conduct that “excludes or disadvantages the products, services, or lines of business of another business user . . . relative to the [platform’s] own”²¹ offerings. While the bill would benefit some large competitors like Epic Games and Spotify, it would harm small app makers like App Association members as well as consumers because they would erode the trust consumers have in conducting digital commerce in the app marketplaces.

H.R. 3816’s prohibitions create a presumption that many platform-level privacy controls are illegal, which platforms could overcome only in especially narrow circumstances. The bill would essentially allow platforms to overcome that presumption only by showing that any measure they take was “narrowly tailored, could not be achieved through a less discriminatory means, was nonpretextual, and was necessary”²² to provide privacy. This construct is in tension with the FTC’s focus on privacy by design and its privacy enforcement against bad actors on the app stores. It is also inconsistent with App Association members’ calls for platforms to expeditiously remove harmful and fraudulent content.²³ In fact, a recent FTC settlement illustrates how a statutory mandate for app stores to allow unvetted software onto smart device operating systems could harm consumers’ privacy and security. On September 1, 2021, the FTC published an initial complaint, along with a unanimously approved settlement, with SpyFone.²⁴ According to the complaint, SpyFone marketed itself as a surveillance app, enabling purchasers to track targets in a variety of ways, including by spying on live location, web history, contacts, pictures, calendar, files downloaded onto a device, notifications, e-mails, video chats, and even social media posts.²⁵ The company explained to its users how to download the app on a target’s device, hide the app so the target would not notice its presence, and bypass Android operating system controls in order to track the target without their knowledge.

Stalkerware apps could easily claim that iOS and Android have similar offerings because their legitimate uses, as marketed, involve parents managing their children’s devices. In this scenario, Android clearly disadvantages SpyFone versus its own offerings by forcing it to go through onerous steps in order for a purchaser to make use of the app. For example, Android forces SpyFone to have its purchasers enable the sideloading capability, which triggers a warning from Android that “[i]f you download apps from unknown sources, your device and personal information can be at risk. Your device could get damaged or lose data. Your personal information could be harmed or hacked.”²⁶ Certainly, these additional steps and a warning like this hurt SpyFone’s business. Likewise, iOS disadvantages SpyFone versus its own offerings because it does not allow SpyFone on iOS devices at all. And the affirmative defense H.R. 3816 provides in cases where a software platform needs to remove an app for violating a law or threatening consumer privacy does nothing to help because as drafted it is so inaccessible as to discourage any sort of reliance on it. The overall effect of H.R. 3816 in the stalkerware context is to create a default rule barring the removal of stalkerware like SpyFone from a platform, as well as any privacy-related barriers that prevent stalkerware from taking advantage of consumers, unless a platform is able to overcome that presumption, likely in narrower forms, on a case-by-case basis.

The bottom line is that taking a nondiscrimination sledgehammer to software platforms’ role in removing bad actors rolls out the red carpet for apps like SpyFone. More importantly, by widening the avenues for fraudsters on app stores, an overbroad Federal nondiscrimination regime would narrow the path for smaller app makers like App Association members. It would also make the FTC’s job in enforcing the statutory prohibition on unfair or deceptive acts or practices that much more

²¹ American Choice and Innovation Online Act (H.R. 3816, 117th).

²² American Choice and Innovation Online Act, Sec. 2(c)(1)(B) (H.R. 3816, 117th).

²³ Statement of Morgan Reed, president, ACT | The App Association, on App Store Review Fraud Scheme (Feb. 11, 2021), available at <https://actonline.org/statements/>.

²⁴ Press release, Fed. Trade Comm’n, “FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data” (Sept. 1, 2021), available at <https://www.ftc.gov/news-events/press-releases/2021/09/ftc-bans-spyfone-and-ceo-from-surveillance-business>.

²⁵ Fed. Trade Comm’n, Complaint, *In the Matter of Support King, LLC, and Scott Zuckerman*, 192 30003 (Sept. 1, 2021), available at https://www.ftc.gov/system/files/documents/cases/192_3003_spyfone_complaint.pdf (SpyFone Complaint).

²⁶ SpyFone Complaint at para. 6.

difficult, as more bad actors enter the fray and less of their activity is discoverable because platforms' hands would be tied. Meanwhile, as consumers adjust to a more fraud and malware-ridden marketplace, they would rationally shift away from experimentally downloading apps with the shortest histories and smallest preexisting distribution in favor of bigger brands. What is now a high trust environment, thanks in no small part to rigorous gating, would then evolve into a no-trust environment, which disproportionately harms smaller companies while benefiting the platform's largest "business users." The effect would be similar with measures like the Open App Markets Act (S. 2710), which takes a narrower approach but still creates a presumption that platform gating functions to protect privacy are illegal.

We urge the Committee to avoid measures like these in their current form, because they would move Federal privacy policy in the opposite direction from where it should be heading. Congress should not *prohibit* (or presume the illegality of) privacy controls that are proven to work; instead, it should *require* companies to adopt privacy protections. Otherwise, Federal law would undo the privacy-protective developments that enable online commerce, forcing consumers to accept a single, more open approach to security, or even worse, bring us back to an early 2000s online experience with fewer options, less meaningful privacy protections, and diminished security.

V. Conclusion

We appreciate that the Committee seeks our views on approaches to bolstering the FTC's ability to address consumer privacy more effectively in the wide variety of industries it oversees and in which App Association members compete. Federal privacy law is overdue for an update to meet the challenges of the 21st century. App Association member companies want stronger Federal privacy requirements in particular, including a single set of national rules governing authorized data processing activities and data security practices. This Committee has made unprecedented bipartisan progress toward agreement on a national privacy law, and we urge that this hearing and further Committee activities help inform that process.

APPENDIX: APP ECONOMY INNOVATORS IN YOUR DISTRICTS

Majority

Chair Maria Cantwell (WA)
Company: Mighty Call

Located in Spokane, Mighty Call is a cloud-based communications and customer service platform founded in 1999. Their virtual phone system is designed specifically for small businesses and remote teams making it easy for teams to connect from anywhere through mobile and desktop apps. Their apps provide unique features like call availability windows, scheduling services, and the ability to mask personal cell numbers, given that privacy is a core pillar of Mighty Call's service.

Senator Amy Klobuchar (MN)
Company: Vēmos

Located in the Twin Cities and founded in 2013, Vēmos is a platform solution for bars, restaurants, and other venues as a one-stop-shop for the digital tools needed to manage and grow their businesses. Operating with only eight full-time employees, Vēmos found a way to harness and present a venue's data in a humanized way, which helps venues understand who their customers are and how to market to them effectively.

Senator Richard Blumenthal (CT)
Company: Pixellet

Located in Stamford, Connecticut, Pixellet is a full-service web and mobile development and design firm with dozens of offered services, including digital marketing and ecommerce. Founded in 2014, Pixellet only has one employee and has served a variety of industries including real estate, health care, financial services, and education, among others.

Senator Brian Schatz (HI)
Company: Smart Yields

Founded in 2015 and headquartered in Honolulu, Smart Yields is an intelligent agriculture software that helps to connect farmers and agricultural researchers to increase crop yield, revenue, and productivity. With fewer than 10 employees, Smart Yields is committed to helping Hawaii meet their commitment to doubling food production by 2030 and other communities achieve similar goals around the world.

Senator Ed Markey (MA)

Company: Podimetrics

Established at the Massachusetts Institute of Technology in 2011, Podimetrics is a medical technology services company that develops hardware-enabled, thermal-imaging solutions to predict and prevent diabetic foot ulcers. The Podimetrics SmartMat™ monitors the temperature of diabetes patients' feet to identify temperature asymmetries that signal the development of a foot ulcer. Coupled with a monitoring service, the Podimetrics Remote Temperature Monitoring System™ uses the wireless SmartMat™ to notify patients and clinicians of temperature asymmetry and inflammation, the first signs of foot ulcers preventing amputations and other health complications.

Senator Gary Peters (MI)

Company: Workit Health

Workit Health is a women-owned digital therapeutics company based in Ann Arbor that is focused on treating addiction. Their Workit Health app connects patients with clinicians and a community, allowing individuals to receive the communal support necessary for addiction treatment, and routine contact with mental health and clinical care givers in the discreet privacy and safety of their home or preferred treatment site.

Senator Tammy Baldwin (WI)

Company: Birdwell Solutions

Founded in Madison in 2019, Birdwell Solutions is a concierge software development agency focused on working with entrepreneurs and startups to build web, digital, and mobile products that help their clients launch and grow their business. With a team that ranges from full stack development to design and project management, Birdwell Solutions is working to foster and support the entrepreneurial community in Wisconsin.

Senator Tammy Duckworth (IL)

Company: Devscale

Founded in 2018, Devscale is a custom app development company with a focus on product strategy. With clients that range anywhere from small to large, Devscale helps their clients through problems in their digital strategy with a trained eye on unique user experiences and a transparent development cycle. Although headquartered in Chicago, Devscale has coders all over the world. They take clients all the way through their creative process; from defining the project through user experience stages and development, to the final rollout.

Senator Jon Tester (MT)

Company: Guidefitter

Headquartered in Bozeman, Guidefitter is an online and mobile platform that connects people with guides, nature experts, and sportspersons for safe and guided natural expeditions and sport including hunting, fishing, hiking, and camping. The platform also allows the experts to promote their business or experience and facilitates payment for merchandise as well as the guided tour or event.

Senator Kyrsten Sinema (AZ)

Company: Devsoft Group

Devsoft Group is a one-man custom development firm founded in 2010. Focused on clients in manufacturing and energy, Devsoft Group works closely with their clients, building web, cloud, SaaS, and mobile and database solutions that meet the unique needs of each client's projects and business needs.

Senator Jacky Rosen (NV)

Company: Pigeonly

Pigeonly is an online and mobile platform that connects inmates with their loved ones. Their services provide a central place to send letters, pictures, cards, and more. Through the platform, families can also call their inmate at a lower cost and stay in touch throughout their incarceration. The company's mission is to improve communication and community for those incarcerated and to encourage families to stay in touch with their inmates by simplifying and streamlining the process.

Senator Ben Ray Lujan (NM)

Company: Snowball

Snowball is an all-in-one fundraising platform that connects users with more than 15,000 nonprofits across the country. The app has two parts. The first is for donors, giving them information about the nonprofits in Snowball's network, donation op-

portunities, and notice of emergency relief needs, and provides a secure place to track donations and save credit card information. The second, for nonprofits, helps to keep track of donors, grow their donor base, and communicate opportunities.

Senator John Hickenlooper (CO)
Company: Atelier

Atelier is a mobile app that allows users to create their own interior design, discover planet-conscious makers of furniture, textiles, art, and more. Through the app, users can design a room and then create 3D images of their designs giving them a clear sense of the finished process. The app also allows users to purchase the pieces they used in their design, supporting small and eco-conscious creators.

Senator Raphael Warnock (GA)
Company: Rimidi

Rimidi creates mobile apps that work directly within electronic health records (EHR) to combine patient-generated health data with clinical data, allowing for patient-specific clinical insights. They have developed a COVID-19 screening application based on the widely accepted Fast Healthcare Interoperability Resources (FHIR) standard for health systems to identify and flag at-risk patients via survey prior to existing appointments. Their tool enables health systems to mitigate the spread of COVID-19, as well as optimize treatment.

Minority

Ranking Member Roger Wicker (MS)
Company: Buzzbassador

Buzzbassador is a management platform for brands that uses ambassadors to promote their products across social media. The platform gives brands the tools to track social media posts, engagement metrics, sales, commission payouts, and more for each of their ambassadors and provides simple analytic reports and a central dashboard.

Senator John Thune (SD)
Company: Infotech Solutions, LLC

Infotech Solutions, LLC is a concierge IT service helping businesses with everything from implementing a new software system or network to maintenance, general IT issues, security, and more. The company also offers an app across platforms that helps their clients troubleshoot IT issues, connect with their IT service team, and more.

Senator Roy Blunt (MO)
Company: Topik

In 2015, two friends co-founded Topik, a mobile blogging application that makes it easy for anybody to create and share blog posts on an easy-to-use mobile platform. Based in St. Louis, Missouri, Topik is completely self-funded and, with only two employees, is set to launch their first mobile app later this year.

Senator Ted Cruz (TX)
Company: For All Abilities

For All Abilities is a software platform that helps companies address and provide for their employees with disabilities. The platform assesses employees and then prescribes and trains them to use individualized supports and accommodations that meet ADA requirements.

Senator Deb Fischer (NE)
Company: Quantified Ag

Quantified Ag is a tracking device and platform to monitor cattle health and enables farmers to quickly remove sick or injured cattle from the rest of the herd to treat them quickly and prevent further infection. The device, worn on the cow's ear, monitors the cow 24/7 and connects seamlessly with the Quantified Ag mobile app allowing ranchers and farmers to easily monitor their cattle throughout the day. Recently acquired by Merck, Quantified Ag built and continues to run the business from Nebraska.

Senator Jerry Moran (KS)
Company: ActiveLogic Labs

ActiveLogic Labs is an innovative digital development agency headquartered in Kansas City with a growing presence across the United States, including an office in the Chicago area. They provide a number of services from web and desktop soft-

ware development to mobile app development, all with a specific focus on user interface design and a seamless user experience.

Senator Dan Sullivan (AK)

Company: StepAway

StepAway is a mobile application to help those with addiction manage their day-to-day and make better decisions about their daily habits to help prevent relapses. The app is primarily centered around those who are unable to seek addiction treatment services but are looking to make a change in their drinking habits. The app helps track daily progress while also giving users insight in their triggers, and provides useful information on how to make different and better decisions related to their alcohol use in a safe and private space.

Senator Marsha Blackburn (TN)

Company: Quiet Spark

Established in 2011 in LaVergne, Tennessee, a wife and husband team founded Quiet Spark after noticing their son's issues with spelling. Their first app was SuperSpeller, an iOS app that makes learning spelling fun for children through learning games and reward features. They have also created other apps that help users keep track of their lives through categories like exercise, reading time, scheduling, homework, and more.

Senator Todd Young (IN)

Company: InGen Technologies, Inc.

InGen Technologies, Inc., is a software consultancy company focused on improving customer experience for their clients and improving data collection and analysis tools to improve their clients' use and understanding of data analytics. The company's mission is to unite all aspects of their clients' digital presence from apps to the web in order to improve overall digital marketing and cohesiveness.

Senator Mike Lee (UT)

Company: 1564B

Located in Salt Lake City, 1564B is a one-man management consulting group that provides advice on marketing and content development as it relates to technical markets, like the Internet of things (IoT). Founded in 2014, 1564B's clients range from startups and growing companies to global corporations.

Senator Ron Johnson (WI)

Company: Xorbix Technologies

Founded over 20 years ago with a location in Hartland, Xorbix Technologies is a custom software development firm helping businesses meet their customers online. They offer a number of services such as full-service custom software development, mobile app development, and general IT consulting.

Senator Shelley Moore Capito (WV)

Company: TMC Technologies

TMC Technologies is an IT services company focused on helping their clients, both Federal and local, with program and project management, scalable system and software engineering, IT infrastructure design and management, and network and telecom services. TMC Technologies has focused a lot of their IT work in their own backyard providing IT services for West Virginia companies, especially small business owners, looking to bring their company into the digital age.

Senator Rick Scott (FL)

Company: Thinkamigo

Founded in 2011, Thinkamigo is an educational app company focused on getting kids excited about writing. Their app, Story Dice, helps give kids ideas for stories, while their apps Lists for Writers and Story Spark help kids lay out their story, build out their characters and plot points, and give them the tools they need to improve their overall writing and story structure.

Senator Cynthia Lummis (WY)

Company: BlackFog

BlackFog is a cyberthreat prevention company that uses a unique combination of behavioral analysis and data exfiltration technology to identify, stop, and prevent future data hacks, unauthorized data collection, and more across mobile and web endpoints. Their services protect their clients and their clients' most sensitive data and privacy while also strengthening their regulatory compliance.

The CHAIRWOMAN. Thank you to all the witnesses. I know there is a vote that has started, so I am going to ask my questions and then have Senator Wicker and Senator Baldwin ask theirs, and then I am going to run and vote, and then we will be back. And hopefully our colleagues who were over voting now will join us.

I want to make something—I heard what everybody said in their testimony. So, but just so we have clarity. So do each of you support more resources at the FTC similar to what we have been talking about as it relates to this reconciliation item on the FTC having more of an enforcement—privacy enforcement authority? Professor Vladeck?

Mr. VLADECK. Yes.

Ms. OHLHAUSEN. Yes, the FTC needs more resources.

Mr. REED. Yes, the FTC needs more resources.

The CHAIRWOMAN. Mr. Soltani? Mr. Soltani, I am pretty sure—do you support more resources like a privacy bureau at the FTC?

Mr. SOLTANI. Correct. Yes, I do.

The CHAIRWOMAN. OK. So the question seems to be, and actually Ms. Ohlhausen, I also heard you also say you were for also first time civil penalties, so—

Ms. OHLHAUSEN. Yes.

The CHAIRWOMAN.—so everybody, I think, also agrees on that, is that right? Everybody agrees on first time civil penalties.

Mr. VLADECK. Yes.

The CHAIRWOMAN. Mr. Reed.

Mr. REED. Yes, as part of a Federal privacy law, I think that it is worthwhile to make that available.

The CHAIRWOMAN. OK, so the issue is that right now we have a volume of cases, and we have a technology gap, and we don't have people to do compliance. So, while we are—what do we need to focus on when we say to the FTC, here are resources?

Definitely want to talk about a new privacy law, but what do we need to focus on to make sure that the resources at the FTC really focus on these issues, when Mr. Soltani mentioned—I mean, my impression is we basically have been using current tools to enforce basically deception in current privacy practices and then having fines for failure—but as Mr. Soltani says, the compliance of that post that seems to be greatly lacking. So, Mr. Vladeck, what does this agency need to do to focus this?

Mr. VLADECK. Well, as I said in my written testimony, the FTC needs resources. One area in which we need resources is being able to hire more technologists and engineers. I don't think the FTC has ever had a cohort as many as 10 technologists on staff. Ashkan was the second technologist we hired, and that was in 2009. So there is really no end to the need by the FTC for resources. But when it comes to enforcement, oversight of existing consent decrees, there is a division within the Bureau of Consumer Protection that has about 45 staff members that oversees more than 1,000 ongoing consent orders or litigated orders imposed by a court. And just the volume of orders that need to be sort of reviewed and subject to reporting requirements overwhelms the ability of staff to do the kind of surveillance of a company under orders that is required.

And so this is one area where, you know, resources are desperately needed because, you know, take a look at Facebook. It is

one of the first real major privacy orders we engaged in. We did not have technologists and staff who could spend time reviewing closely what the company was doing. And that is an endemic problem. And it is going to be an enduring problem unless Congress devotes more resources to the FTC.

I was a triage nurse for four years, really. That was what I did. I tried to reallocate resources to the most dire, you know, to the most dire function that the FTC could—

The CHAIRWOMAN. Well, I think that—I think I want to ask Mr. Soltani about this, because I worry that people are paying the fines and then going back to practices, knowing that we don't have time for compliance. And this is everywhere, you know, in the Federal Government. Senator Wicker and I had to work very hard on aviation reform, which was the same issue of what did the FTC—I am sorry, the FAA have as far as technologists to really understand the technology that they were reviewing.

So we need an upgrade across the Federal Government, but clearly, if we want compliance on safety—Mr. Soltani, since you mentioned a broad group of people, but don't we just need basic people who understand software operations and technology?

Mr. SOLTANI. It depends on the scope of the order. But absolutely, I think having expertise in, for example, the matters under order. So Facebook has a compliance program that they rely on a third party assessor for, and in some cases the FTC doesn't even automatically receive those. They have to request those assessments.

But then you, as David mentioned, you need not only resources, but the right resources that can actually attest to whether these assessments are accurate, are done in the right scope, or even whether the assessor has the skills necessary. A lot of them are just checklists. So I think we need expertise, for example, on data security, APIs assessments in those groups overseeing the orders, compliance with the orders.

The CHAIRWOMAN. Yes, I would—anyways, I would like to see a more formal list from somebody, but we will get—we will keep moving on the process and then seeing—yes, Senator—I mean, Mr. Vladeck.

Mr. VLADECK. Yes, can I add just one quick thing. You know, in most privacy cases there is no fine or nothing in terms of redress for the first violation. There is no original fining authority because privacy harms, you know, are not monetary. You know, first—you know, the first violation is basically sort of, you know, consequence free other than the ongoing order.

The CHAIRWOMAN. I will get to you, Mr. Reed, but I—Senator Wicker, go ahead and then I will get back to you when we come back. And then Senator Baldwin.

Senator WICKER. Get your steps in, Senator Cantwell. Thank you very much. First of all, I have in my hand an article from today's *Wall Street Journal*, "FTC Weighs New Online Privacy Rules" by John D. McKinnon and Ryan Tracy, and I ask unanimous consent that it be placed in the record at this point. Hearing no objection—thank you.

[The information referred to follows:]

FTC WEIGHS NEW ONLINE PRIVACY RULES

Agency is looking at strengthening rules that govern how digital businesses collect user data



The FTC has signaled interest in taking further action on digital privacy concerns, particularly with regard to children.

PHOTO: GABRIELLA DEMCZUK FOR THE WALL STREET JOURNAL

By John D. McKinnon and Ryan Tracy—Updated Sept. 29, 2021 2:00 pm ET

WASHINGTON—The Federal Trade Commission is considering strengthening online privacy protections, including for children, in an effort to bypass legislative logjams in Congress.

The rules under consideration could impose significant new obligations on businesses across the economy related to how they handle consumer data, people familiar with the matter said. The early talks are the latest indication of the five-member commission's more aggressive posture under its new chairwoman, Lina Khan, a Democrat who has been a vocal critic of big business, particularly large technology companies.

Congressional efforts to assist the FTC in tackling perceived online privacy problems was the focus of a Senate Commerce Committee hearing Wednesday. If the agency chooses to move forward with an initiative, any broad new rule would likely take years to implement.

In writing new privacy rules, the FTC could follow several paths, the people said: It could look to declare certain business practices unfair or deceptive, using its authority to police such conduct. It could also tap a less-used legal authority that empowers the agency to go after what it considers unfair methods of competition, perhaps by viewing certain businesses' data-collection practices as exclusionary.

The agency could also address privacy protections for children by updating its rules under the 1998 Children's Online Privacy Protection Act. And it could use its enforcement powers to target individual companies, as some privacy advocates urge.

The FTC might choose not to move forward with any major privacy initiative. And action could be delayed as agency Democrats wait for confirmation of President Biden's newest nominee to the commission, privacy advocate Alvaro Bedoya.

But since taking office June 15, Ms. Khan has made a number of moves to lay the groundwork for potential rule making, including by voting with the FTC's two other Democrats to change internal procedures to expand her control over the rule-writing process. Mr. Biden has *ordered the FTC to look at writing competition rules* in a number of areas, including "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."



Democratic FTC Chairwoman Lina Khan has taken a number of steps to lay the groundwork for potential rule making.

PHOTO: GRAEME JENNINGS/PRESS POOL

This week, the progressive-leaning advocacy group Accountable Tech petitioned the agency to ban “surveillance advertising” as an unfair method of competition, defining the practice as targeted advertising based on consumers’ personal data. As an example of the harms that an alleged lack of competition among online platforms can cause, the group cited a recent *Wall Street Journal* article about the impact of Facebook Inc.’s Instagram app on teens’ mental health.

“The ability and incentive to extract more user data to unfairly monetize, even at the expense of children’s wellbeing, has proven too great a competitive advantage for dominant surveillance advertising firms to pass up,” the group’s petition said.

Facebook has said it faces stiff competition and that the *Journal* mischaracterized internal research on Instagram’s impact. It said this week that it was *pausing work on a version of the photo-sharing platform* designed for children under 13.

If the FTC decides to write a privacy rule, it would first have to publish a draft and seek public comment. In some circumstances, the law requires the agency to take additional, time-consuming steps such as asking for public input before even publishing a draft of a proposed rule.

Such efforts could get a boost from congressional Democrats seeking more funding for the agency.

Sen. Maria Cantwell (D., Wash.), who chairs the Commerce Committee, argued Wednesday for augmenting the FTC’s resources to better address problems of the online economy.

“The truth is that our economy has changed significantly, and the Federal Trade Commission has neither the adequate resources nor the technological expertise at the FTC to adequately protect consumers from harm,” she said in her opening statement.

Some Republicans said it wouldn’t make sense to add significant new funding to the FTC without passing new laws.

Earlier this month, House Democrats proposed giving the FTC a \$1 billion budget to fund a new bureau dedicated to overseeing “unfair or deceptive acts or practices relating to privacy, data security, identity theft, data abuses, and related matters.” That proposal will be subject to negotiations as the narrowly Democratic-led Congress looks to pass a broad new spending plan this fall. Meanwhile, several Senate Democrats wrote to Ms. Khan on Sept. 20 asking her to write rules protecting consumers’ privacy.

The lack of a broad Federal law protecting consumers’ privacy has become a bigger concern for advocates as online platforms and others have amassed vast troves of consumers’ search data and other information. Many privacy advocates are *par-*

ticularly worried about children, who can be more vulnerable to targeted online advertising and *attention-grabbing algorithms*.

Legislation to establish broad-based Federal privacy protections *has stalled again in Congress* this year over a range of concerns. Efforts to update an existing 23-year-old Federal privacy law covering younger children haven't gained significant traction among lawmakers.

Critics say the Children's Online Privacy Protection Act and the FTC-written rules that enforce it are ineffective and out-of-date, concerns that have helped lead the agency's newly empowered Democrats to focus more on taking further action on privacy.

"I think it's a really, really important area for attention," Democratic FTC Commissioner Rebecca Slaughter has said of adopting broad-based privacy rules. She said at a July congressional hearing that a potential rule could target suspected online harms to children, adding, "That is an issue that's near and dear to my heart."

Ms. Khan and fellow Democratic commissioners indicated at that hearing that the agency would be giving more attention to how platforms might be abusing children's privacy, as many kids have spent more time online during the Covid-19 pandemic. Democratic Commissioner Rohit Chopra added that the FTC should examine the underlying business models that can lead to privacy abuses.

Republican Commissioner Christine Wilson has become an advocate for Federal privacy legislation, saying that consumers don't understand how their data is collected and monetized, creating what she terms a "market failure."

"Without this information, they cannot analyze the costs and benefits of using different products and services," she said last week at Duke University. "And the risks to consumers from the unchecked collection of their data have intensified in recent years."

Write to John D. McKinnon at john.mckinnon@wsj.com and Ryan Tracy at ryan.tracy@wsj.com

Appeared in the September 30, 2021, print edition as 'Federal Trade Commission Weighs Stronger Online Privacy Safeguards'.

Senator WICKER. And it starts out, the Federal Trade Commission is considering strengthening online privacy protections, including for children, in an effort to bypass legislative logjams in Congress. Ms. Ohlhausen, have—this just came out this morning. Have you had a chance to read that?

Ms. OHLHAUSEN. I haven't had a chance to read that. But I have heard some encourage that the FTC proceed through rulemaking.

Senator WICKER. OK, and I take it from your testimony that you don't think that is a very good idea?

Ms. OHLHAUSEN. I don't think it gives the FTC the necessary statutory authority from Congress.

Senator WICKER. As you pointed out in your testimony. Mr. Vladeck seems like Ms. Ohlhausen makes a pretty good case that really the FTC should wait for Congress no matter how much of a logjam we have, that really is ideal that Congress act on this rather than the agency. What do you think about that?

Mr. VLADECK. Well, I agree that Congress is the right body to finally decide what the law should be. I completely agree with that. I am not sure—and you know, and I don't think an FTC rule is anyone's first choice.

Senator WICKER. And she makes up—she makes some pretty good points about what an FTC implemented rule would lack in terms of a force and effect. Do you agree with her on what she said in her statement?

Mr. VLADECK. No, I think she's incorrect about the preemption issue. I think in the FTC rule promulgated under Section 18 would preempt State law that conflicts with the FTC rule. There is a lot of Supreme Court jurisprudence on preemption. That one issue, I think Ms. Ohlhausen is incorrect.

Senator WICKER. That is a pretty powerful agency that can do that. What do you think, Mr. Reed? Have had—have you read the article? Anyone read the article?

Mr. REED. Well, we have jumped off on to the rulemaking. I think when it comes to the protection of children online, we have been a strong supporter of the Children's Online Privacy Protection Act. One of the things, though, that I was, and I will repeat this for the chair is, it is worth noting that on all of these rules, we run into a situation where we are all talking about compliance.

To me in a small business capacity compliance means lawyers. That doesn't mean developing products. That doesn't mean people doing the job that they need to do. So what really the FTC needs to have as part of this resource is to make sure they are doing a better job educating people what the rules are, how you follow them, what the expectations are, and get back some of that trust. Because if we are only focused on compliance, that means I am hiring a lawyer, not the other.

On onto your question about a patchwork of State laws, somebody asked me earlier said, well, is a patchwork of State laws going to—doesn't that create a floor, not a ceiling? And I said from a small business perspective, that turns the floor into lava, and you are hopping from couch to couch to trying to figure out where you comply and how you comply. While I understand that there is jurisprudence, as Professor Vladeck said, from a small business perspective, the cost of figuring out where you sit on that jurisprudence is incredibly expensive and time consuming.

So, no, I think preemption is absolutely key for the small business success. And we can't depend on a hopeful Supreme Court decision down the road.

Senator WICKER. And perhaps Mr. Soltani can answer on the record because that clock seems to keep ticking. Let's talk about the inclusion of a private right of action in data privacy legislation. Oftentimes, a private right of action hinders innovation, consumer choice, and ends up benefiting trial lawyers rather than consumers. For the record, and we will start again with Ms. Ohlhausen, and talk to all four of you.

How would a broad private right of action and data privacy legislation impact member companies, particularly small app developers, and what do you think about a private right of action where consumers can recover actual monetary damages where an individual has suffered concrete harm? Let's start with Ms. Ohlhausen but we'll take time for all four of you.

Ms. OHLHAUSEN. So I would support a private right of action that allows a consumer to get actual damages. I think concerns, you know, are appropriate for a very broad type of right of action as the way we have seen that used when it has been in other statutes, where it really hasn't serve consumer interests well and it is certainly been a big burden on businesses, including small businesses, who have to spend a lot of money, you know, defending against—

Senator WICKER. What would you—what would you allow and what would you not allow? Can you help us make a distinction there?

Ms. OHLHAUSEN. Sure. So I have some concerns about having something that has high punitive damages for an initial violation of the Act, particularly of something that, you know, doesn't have like, you know, a bad intent. If you had something that was, you know, really focused on repeated or egregious violations, that focused on making consumers whole and protecting consumers going down the road, I think that is the appropriate focus for a private right of action.

Senator WICKER. Mr. Vladek.

Mr. VLADECK. I think private rights of action are essential to enforcement, but I think there are ways of addressing the concerns that you and others have raised. So, for example, the Federal Privacy Act has a private right of action. It only permits nominal damages unless there are actual damages. And under the Equal Access to Justice Act, it curbs the amount of attorney's fees that can be recovered.

And so there are ways of both providing a right of action which would be essential to real enforcement but minimize the kinds of concerns that you and my colleagues here today have raised. Look at the Federal Privacy Act. It has been in effect since 1974. It has worked quite well, but it has a private right of action. It allows nominal damages, and it curbs attorneys' fees.

Senator WICKER. Mr. Reed, what about your small members?

Mr. REED. So, Professor Vladeck mentioned some guardrails, but I think if we are going to have a private right of action, guardrails are the key aspect. Obviously, injunctive relief—injunctive relief would probably be ideal. But if we are limiting it to just monitor actual monetary damages, not statutory, I think the two problems small businesses are going to see is without a period to cure, you run the risk of I didn't respond to that e-mail in 30 days, I responded to it in 31 days.

That should not lead to a sue and settle situation where I have got to pay someone—I have got to pay someone \$50,000 for that. So there has to be a period of cure. The other thing that we have heard from everybody is the concept of C-enter. There has got to be some kind of intent behind it. A missed deadline for responding to a request shouldn't be the kind of thing that leads you into an expensive court case. So guardrails are the key aspect.

Senator WICKER. Mr. Soltani, is a period of cure OK with you?

Mr. SOLTANI. Yes, I think that the cure provision does provide some guardrails, as Mr. Reed outlined, and we have that in California. I will say that those guardrails, though, need to be specific, not just based on the size of the company, because oftentimes small companies will actually affect and reach millions of consumers and handle sensitive data like health information or period tracking apps.

So I am not sure that just the size of it alone—it has to be a consideration based on, as others have said, the nature of the harm and the severity if the information does breach. You know, at the end of the day, the private right of action makes up for the concern if there is not enough enforcement capacity. So I think as long as there are ways to ensure that the laws and regulations are properly overseen and enforced and there is resources to do so, I think that will balance the private right of action as well.

Senator WICKER. Thank you. Senator Baldwin, take the gavel and take 8 minutes if you need to. We will hold up—
[Laughter.]

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

Senator BALDWIN. I have noted in previous hearings in this committee about data privacy that I am not sure that my constituents really differentiate between a company's decision to use their data or give it to others in ways that they didn't expect or agree to, and a company's failure to keep that data secure from third-party criminals who steal it. Unfortunately, since our last hearing on this topic, we have seen a lot more large scale data breaches and ransomware attacks that endanger consumers' personal and financial information and threaten the operations of critical businesses and services.

So I am pleased that the legislative proposals introduced by the leaders of this committee tackle the issue of data security as part of the broader data privacy issue. Ms. Ohlhausen, during your tenure at the FTC, the agency dealt with a number of major data breaches. How critical do you believe it is that Congress tackle data security alongside sort of hand in hand with data privacy issues? And what in particular is the—is it most important for Congress to do in the data security lane?

Ms. OHLHAUSEN. Thank you, Senator. I think you are correct that there is a fine distinction between data privacy and data security, but they are very closely related. And I think it is important that Federal legislation tackle both.

And some of the provisions that have been in the bills require companies to have processes in place to ensure that the data is protected, that they also might be subject to fines if they don't, because that is—you know, as my colleague, Mr. Vladeck said, sometimes the harms from a data breach aren't necessarily financial harm.

Sometimes they are, but they aren't always. And so you want to be able to have the right incentives in place for companies to take those protections. And I think legislation that looks at both privacy and data security helps kind of cover both sides of that.

Senator BALDWIN. Thank you. All of you have testified about the need for the FTC to have greater resources and in particular, technologists, engineers. And so I want to—I had a question on that, but you pretty much put that on the record. I do want to ask something more specific about it, though, and I will direct this to Mr. Soltani. In your testimony, you recommended that the FTC grow its staff of technologists, provide them with more competitive pay, allow them to engage in meaningful work that would not prevent them from seeking future employment elsewhere.

While I agree, and there seems to be a strong consensus on the panel that the Commission needs substantially more staff, resources, and authority to effectively address data privacy and security, I also have long standing concerns about revolving doors—a revolving door between Federal regulatory agencies and the industries that they regulate.

So how would you suggest we go about approaching that, strengthening the FTC's ability to effectively engage with an ever changing and expanding technology sector while also trying to avoid industry capture?

Mr. SOLTANI. Thank you, Senator, for the question. Absolutely in agreement with you regarding the revolving door we see, and this committee is intimately familiar with staff going to large tech companies and working after the fact once they gain that expertise here. The comment in my testimony and I have coauthored a paper on this, has to do with the way contract rules apply to technologists.

And I also said in my testimony, often technologists—when I was at the Commission, I worked on nearly every case at DPIP at the time. So I was working hands on, on many cases. And so as such, it essentially creates enhanced conflict rules, particularly based on the way the FTC interprets their conflict authority. And furthermore, they apply those conflict rules not just to working with the companies that are under order but working with other enforcement agencies.

For example, I worked firsthand on the Facebook matter in 2010 as one of the lead investigators, technologists in the matter. I was prohibited by the FTC from helping a multi-State AG action on the same matter because they considered that to be in the conflict rules even though it was on the same side of consumer protection, and it would be essentially seeking injunctions or remedies that the FTC themselves didn't seek.

So I think there is some work that needs to be done, but absolutely with the focus that this can't be a revolving door. In the same way that we want to prevent a revolving door, not just for staff attorneys, but for Commissioners as well.

Senator BALDWIN. Thank you.

The CHAIRWOMAN. Thank you, Senator Baldwin. I know Senator Fischer is here, but you are allowing your colleague, Senator Moran, for a time constraint, sensitive issue to go remotely ahead of you. So, thank you. Senator Moran. Senator Moran, are you available? Maybe he already had to depart for his—well, we will give it a minute here. Give it a second. See if we can get it corrected. If not, would it be OK if we went to Senator Tester, and then back to Senator Moran, is that OK? OK, Senator Tester.

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

Senator TESTER. Well, goodness, thank you. This is a question for—actually, it is a question for the panel. We have witnessed the FTC fine some larger tech companies a pile of money in my book, billions of dollars. Number one, do you think this enforcement is effective? And number two, if you don't think it is effective, because, quite frankly, I think it is a drop in the bucket to some of these companies, but if you don't think it is effective, what should the FTC be doing? We will start with you, Mr. Vladeck.

Mr. VLADECK. You know—

[Technical problems.]

The CHAIRWOMAN. If you could turn your microphone on, I am not sure, or pull it closer.

Mr. VLADECK. Thank you. I think \$5 billion actually is a bucket of money. And having litigated cases for 45 years, I doubt, seriously the FTC would have gotten that kind of civil penalty in litigation. But here's the problem. For most privacy violations, there is no financial, you know, harm to the company. They don't pay a penny in most privacy violations. Why? Because it is not money. And the FTC, of course, redress authority was clipped by the Supreme Court in AMG. But for first time violators, the only real sanction is an ongoing consent decree.

And as—we talked about this a little earlier, Senator Tester, but part of the problem is the FTC has got 1,000 companies and people under order. And monitoring those consent decrees, it takes a lot of time and resources, which the FTC lacks. And so the real problem is once you get a company under order and during my tenure at the FTC and Maureen's, we got a lot of these companies under order.

The real question is, does the FTC have the resources to make certain the company is following the consent decree? And the answer to that question is plainly no.

Senator TESTER. Yep.

Ms. OHLHAUSEN. So I agree, I think \$5 billion is a big fine and is actually much larger than—we often hold up Europe as sort of this paradigm for privacy and it far dwarfs anything they have ever obtained there. But I think the other part that you need to look at is the conduct obligations that are in that order.

And so when you look at legislation and the ability to impose some of those kinds of obligations on all companies, I think that is why Federal legislation could be really a good path forward, not just unfair and deceptive acts and practices enforcement, which, again, I think the FTC has done a good job with, given the limitations that that has.

Mr. REED. So from the small business perspective, \$5 billion is a lot of money. However, what you are really asking is, did it create behavior change? And the practical mention is we keep talking about compliance. Well, without Federal legislation, you are never going to see—you are never going to see behavior change, because what the companies are doing is they are looking at what the length and breadth of the law are and figuring out how close they can come to the line to comply and then figure they will fight it out in court and delay it.

So until the Congress comes in and steps in and says this is what is appropriate, this is what people—what their expectations are, and restore some trust to the system, then it is always going to be a matter of \$5 billion. So as Ms. Ohlhausen said, really, it is up to Congress to actually give the FTC the tools they need. But if you want behavior change, it starts with you.

Senator TESTER. Mr. Soltani, would you like to comment?

Mr. SOLTANI. I would agree with what the previous panelists have said. Indeed \$5 billion may be a lot of money depending on the company, however, the kind of the core behavior change comes about not only from the fine, but also any injunctions or restrictions that are imposed on the company.

In the case of the—from the Facebook settlement, not only were there very limited injunctions on the behavior of the company, the

settlement indemnified the company for all violations prior to the settlement date, which there is some evidence that there was a number of other ongoing violations at the time, which the FTC then loses its ability to oversee or enforce.

So I think in addition to statutory fines, I think it is important to have strong, meaningful injunctions, which then the agency can, in fact, enforce. And that goes to the resource question as well as the authority question.

Senator TESTER. Several of you, if not all of you, have talked about the fact that they don't have—the FTC does not have enough money to do what we think they should be doing. The House marked up a bill that gives them basically \$100 million a year for 10 years to create a new privacy bureau. I am curious, and I would love to ask you all this question, but I only got 13 seconds left. So I will just ask you, Mr. Vladeck, since you are closest to me, what should we be looking at as far as the funding level for the FTC?

Mr. VLADECK. I think an additional \$100 million a year is a good start. It would move the FTC to parity with some of its other sister agencies, but I am not sure that is actually enough. I mean, when we start—the first time we see Google, they had 600 lawyers.

Today, I don't know, probably over 1,000. You know, we are not ever outgunned, but we are always outmatched in terms of resources. And as the tech sector grows and it is the most dynamic sector of our economy, the FTC is going to need resources commensurate with that. So I think \$100,000—\$100 million is a good start, but I don't think that is the end of the story.

Senator TESTER. Thank you. Thank you, Madam Chair.

The CHAIRWOMAN. Thank you, Senator Tester. Senator Moran, are you now available? Senator Fischer.

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

Senator FISCHER. Thank you, Madam Chairman, and to our witnesses for being here today. This committee has had productive discussions on data privacy in recent years. And on several occasions, we have heard directly from FTC Commissioners past and present, and from both parties for that matter. What struck me from those conversations was that while many Commissioners had different recommendations, they consistently pointed to one area of agreement, and that is the need for Congress to clearly define authorities and boundaries for FTC rules in statute. Commissioner Ohlhausen, do you think it makes sense for lawmakers to throw as much as \$1 billion at a new privacy bureau as some are trying to do without passing corresponding legal authorities for FTC enforcement?

Ms. OHLHAUSEN. I think you really need both. You need more resources financially and you need stronger statutory guidance and clarity for the FTC to enforce. Because if it keeps trying to enforce in a way that doesn't quite match up with the authority Congress gave it, it is always going to be at a disadvantage.

Senator FISCHER. Without the right legal tools provided by legislation, I am afraid that this funding would waste taxpayer money on unsuccessful agency litigation that would ultimately fail, and it is not going to protect consumers in any way.

Mr. Vladeck, I noticed in your testimony you mentioned digital harms that are related, but beyond the immediate privacy space, such as dark patterns. I am working to reintroduce the Detour Act with Senator Warner, prohibiting the use of dark patterns that trick consumers into giving consent online. How do you think that legislation addressing these manipulative user interfaces could improve the FTC's ability to protect consumers online?

Mr. VLADECK. Well, first, you know, the FTC protects consumers online largely through litigation. And unless the FTC has the resources that it needs today, the FTC is not going to be able to do that. In terms of dark patterns, there is a difficult—there is a really difficult First Amendment question there. The question is, what is the difference between advocacy and manipulation?

And I think the trick that you and your colleagues are going to have are going to be to craft legislation that gets out—really gets after the kind of manipulation that you are worried about without, you know, without trenching on First Amendment rights. So I applaud what you are doing, but I think you have a very difficult road ahead of you.

Senator FISCHER. I am also very troubled by the recent *Wall Street Journal* reports that describe Instagram's mental health effects on its users, particularly young girls. This follows our concerns about Facebook previous mood studies that they did to manipulate users' emotions that came to light in 2014.

The DETOUR Act seeks to address consumer harms like these, as well as by banning online behavioral studies without informed consent and banning certain dark patterns aimed at children. How would you tie in your previous comments on First Amendment issues to be careful about, to be cautious about, on those instances?

Mr. VLADECK. I am deeply troubled by the *Wall Street Journal* reports about Facebook. You know, anyone who has ever raised children, I think, particularly in this digital age, should be worried about it. I think the Constitutional issues definitely are less substantial when you are trying to protect minors.

And you know and the FTC enforces COPPA. I would like to see changes to COPPA. The COPPA statute is very difficult to enforce because of the actual knowledge standard. I would hope Congress could wrestle with that question as well. But I agree with you, we need tighter regulation to protect our kids.

Senator FISCHER. How can we aid you in that enforcement? You know, when we are looking at consumer harm, can you give me a couple of examples of areas that you think we need to focus on in order to aid you in that enforcement? What are some of your ideas? What do we need? What do you need?

Mr. VLADECK. Well, the first—if we are talking about children, COPPA needs to be revised. I helped work on the 2000, you know, 2011, 2012 rethink of COPPA, and we were constrained by the statute. The hardest problem for the FTC is the actual knowledge standard that it requires us to prove from the get-go that an app developer website actually understood that it was tracking children, even though, you know, there is a lot of circumstantial evidence that would have proven constructive knowledge.

So the first thing I would do about COPPA is change the standard from actual knowledge to constructive knowledge. The second

thing I would do is get rid of the safe harbor programs. They give people one serious bite at the apple without FTC oversight. I do not think the Safe Harbor program has worked particularly well. And the last thing is I think there needs to be a rethink about the age limit. I don't know whether, you know—Senator Markey is not here. I don't know—oh, oh, there you are, Senator.

The CHAIRWOMAN. He is pretending to be a staffer.

Mr. VLADECK. Oh, I apologize.

The CHAIRWOMAN. He is so knowledgeable. He is at the staff level of knowledge. He is so smart.

Mr. VLADECK. Well, I mean, in some ways he was remarkably prescient. The statute goes back to 1999. But I think that we need to rethink what the right age is.

Senator FISCHER. Thank you. Thank you, Madam Chairman.

The CHAIRWOMAN. Thank you, Senator Fischer. Is Senator Klobuchar available? She may—she has been trying—

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

Senator KLOBUCHAR. Can you hear me, Madam Chair?

The CHAIRMAN. Yes. Yes, Senator Klobuchar.

Senator KLOBUCHAR. Thank you, Madam Chair. Thank you. I am going to Senator, a former Senator wife's funeral, and I apologize for just being on the phone here. I am on the bus, but I really wanted to be part of this important hearing. And I thank you for your leadership, Senator Cantwell and so many others.

Mr. Soltani, in your testimony in opening, you highlight probably FTC's Division of Privacy and Identity Protection has only about 40 attorneys as compared to other countries' data protection agencies such as Germany, with one-quarter of the U.S. population, with nearly 745 staff. You also note how a new FTC privacy bureau would provide the agency with the resources it needs. Can you elaborate on how this bureau will help build upon the agency's work to protect consumer privacy?

And I would also add to that, Senator Grassley and I, of course, have a bill that would help both the FTC and DOJ antitrust, when it comes to antitrust enforcement that is passed the Senate. And there is also efforts to beef up the resources on that side of the work, which I think does lead into privacy because, you know, there is no incentive to do a lot on privacy when there is only one competitor in a dominant platform. So could you address both things, Mr. Soltani? Thank you.

Mr. SOLTANI. Absolutely. I think, as I said before, regulation and even Section 5, without adequate enforcement and oversight, is just dead letter. And effectively the enhanced—kind of the creation of this new agency plus the staffing expert resources—sorry, the creation of this new bureau with staffing of key resources will help the agency not only kind of enforce and oversee the myriad of harms we are concerned about, but in fact go after a number of companies rather than just one or two at a time. And as you know, often these matters take years to complete.

So it gives the ability to, for the agency to actually oversee more of what you are all concerned about. To your second point, absolutely, privacy and antitrust are deeply related. I don't think you

could solve one without solving the other. And I do think that efforts to try to deal with some of the market failure resulting in some of the privacy abuses is critical.

Senator KLOBUCHAR. Thank you very much. Professor Vladeck, I recently held a hearing in antitrust about consumer data and how literally so much information feeds into the profiteering of the tech companies that's off of consumers' back. I think Facebook makes their own reports \$50 bucks a quarter from each user in America. And so could you talk about how a large data set held by a small handful of companies can raise competitive concerns such as barriers to entry?

Mr. VLADECK. Thank you. Thank you, Senator. I do think these enormous reservoirs of personal data, which are constantly being updated frictionlessly with no cost to the companies, is an enormous asset that is a barrier to entry and is a barrier to rivals trying to replicate these kinds of data banks. And so I think that, you know, I agree with you that these aggregations of enormous amounts of sensitive personal data are an enormous asset. Of course, the accounting industry hasn't really caught up to this, but we have at the FTC. And, you know, the frictionless acquisition of personal data on an ongoing basis is an enormous advantage in this marketplace and will freeze out rivals.

Senator KLOBUCHAR. OK, thank you. Last question. Ms. Ohlhausen, there is a lot of concern about health technologies. I have done work with Senator Murkowski on this and many others, whether it is tracking apps, whether it is Halo, you name it. Could you just briefly talk about that? Thank you.

Ms. OHLHAUSEN. Thank you, Senator. Your question was a little hard to hear. So—

The CHAIRWOMAN. Halo. Halo Technology.

Ms. OHLHAUSEN. Halo Technology? OK, I am not actually familiar with Halo Technology, so—but I will say the FTC has been active in paying attention to apps that are surreptitiously tracking consumers. They recently brought some enforcement actions in that area. I think that that is something that, you know, going back to our time with David, the Golden Shore's flashlight app, where they were collecting data. You know, they said it was a flashlight, it worked as a flashlight, but it collected data and consumers didn't know that.

So I think—designer wear, yes. So there is—so I think that that is an area where the FTC has been active, continues to be active, and certainly any legislation should address those kinds of concerns as well, because if there is sensitive data that is being collected unknown to consumers, you know, that is that is an issue. There should be an opt-in consent there.

The CHAIRWOMAN. Thank you. Thank you, Senator Klobuchar. Senator Scott.

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

Senator SCOTT. First of all, I want to thank Chair Cantwell for hosting this important hearing. Online platforms and big tech companies actively track, collect, and sell the data of Americans, often without their users' knowledge or consent. I think all of us are

alarmed by this, and it is an infringement on Americans' privacies. Our job in Congress is to hold these companies accountable and protect the rights of all Americans.

There are privacy policy frameworks in the EU and states like California that purport to give more ownership of data to users. But I am concerned that these frameworks do not actually give individuals more control of their data and burdened small businesses do not have the legal and compliance resources of big tech. Congress needs a thorough review and reform existing privacy law to make sure Americans have more control and transparency about how their data is being used, as well as the ability to protect their data. I have a bill, the DATA Act, which would require big tech platforms like Facebook, Snapchat, and Twitter, to receive expressed consent to use American's personal information and also provide a recourse for Americans if the right to privacy is violated.

I think this bill is a step in the right direction to give Americans greater transparency and control of their personal information. To all the witnesses, thank you for being here. If we pursue Federal legislation, how can Congress ensure it is carefully crafted to ensure that small businesses do not face burdensome new requirements?

Mr. REED. Well, I guess as—from the small business perspective, I will start, Senator Scott. There are some basic guardrails that need to be in place around any private right of action. Specifically, we talked about it earlier, the baseline concepts have to be that it cannot be a private right of action that would result in, for example, a small business getting an e-mail from someone and responding to it in 31 days instead of 30 days.

We need a period of cure. We need to be held to the point where there was no intent to harm and there is a way to clarify or fix the problem and get right with our consumer, because at the core, the small business needs the consumer trust. We don't have the big brands of a Facebook. We actually need our consumers to trust us. And so setting up a system of PRA that becomes sue and settle, where the cost of going to court to defend myself is \$500,000 but paying off the lawyer \$50,000 becomes a cost of doing business.

So I would say that, as you have heard from all the panelists, there is support for some kind of PRA, but it needs to have guiderails to respect the realities of small business. And those start with making sure that we can fix the problem and make sure we are on the right side of trust with our customers.

Ms. OHLHAUSEN. Senator, I also agree that we need to come up with a system that doesn't overburden small business. Regulatory complexity makes it very difficult. So having a uniform national law that sets out clear standards, clear obligations, I think will go a long way toward reducing that complexity for small businesses.

Mr. VLADECK. Senator, I share your concern about overburdening small businesses, but one of the things that we need to take into account is in the digital space, a small business can create massive harm. And the FTC saw cases like that. And so I do think that, you know, you have a fair point, but you need to craft legislation that, you know, that is commensurate with the amount of harm that can be caused. And so there were cases that we litigated when I was at the FTC, frost wire, designer wear, where there were app

developers that could really just create massive harm. And so we need to—we need to balance those two factors, Senator.

Mr. REED. And just to followup, I actually agree. I think small businesses can have data pools that are very significant and therefore the harm that they cause can be serious. The questions of the ability to cure, the ability to solve the problem, the ability to regain trust is true regardless of size, but it is more profoundly felt by small businesses. It is one of the reasons why we need preemptive Federal legislation to help us, you know, get the trust of our users.

Senator SCOTT. Thank you. What can we—how can—

Mr. SOLTANI. Senator—

Senator SCOTT. Go ahead.

Mr. SOLTANI. If I may. So, I agree with you, and I agree with the previous panelists that in fact the burden on small business and innovation should be considered. In California, we have a threshold which considers not only the company size, for example, if it has an annual gross revenue of over \$25 million, but also the amount of data that it sells or shares, for example, over 50,000 consumers, which is updated in the CPRA. The—you know, to Professor Vladeck's earlier point, oftentimes small businesses may still handle and deal with a lot of personal information, sensitive personal information.

So we need to have a framework that is flexible enough to deal with the compliance issues as Mr. Reed just pointed out, but also deal with the harms that can come about around a fast, rapidly growing business. Think about Twitter. When the FTC brought the order against Twitter, they were at that time perhaps a small business, but that impacted quite a lot of people's lives in 2009, 2010.

Senator SCOTT. Thank you, Chair Cantwell.

The CHAIRWOMAN. Thank you. Thank you so much. Senator Moran tried to join us earlier and now he is available. Senator Markey is it OK if—he is trying to get to the same funeral our colleagues are trying to attend, and I—we all mourn the loss of Evan Bayh's wife, and so I guess they are having a memorial service this morning for her. So, Senator Moran, would you like to try to connect here?

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

Senator MORAN. Chairman, I thank you very much, assuming you can hear me. Thank you for your assistance in allowing me to testify, but it is hugely an important issue to me and to the country and issue that I and you and Senator Blumenthal and Senator Wicker have spent a lot of time on. I have a couple of questions. I guess I will begin with Commissioner Ohlhausen and Mr. Vladeck. There seems to be significant agreement on what a comprehensive data privacy bill should include, but there is still a few sticking points, and they are certainly difficult ones. One of those serious ones is the remaining issue of whether to include the private right of action. And if so, what form should that take? Where do you believe we can find common ground on this particular issue? Commissioner.

Ms. OHLHAUSEN. Senator, thank you for your question. I do think there can be common ground found on private right of action, as

we have—I think fellow panelists have also talked about, having a private right of action that is very focused, that does not invite abusive litigation. That is focused on getting actual redress to consumers rather than just generating attorneys' fees. So I think that, you know, that and my colleague suggested the Federal Privacy Act as a model and definitely would want to take a look at that.

Senator MORAN. Thank you.

Mr. VLADECK. Let me just quickly add one thing. A privacy bill needs to be enforced, and the only effective real mechanism of enforcement are private right of actions. Now, there are concerns about frivolous litigation or excessive costs. There are statutes that deal with that kind of question. The Privacy Act is just one, but there are ways of limiting recoveries to nominal damages and actual damages and to cap attorney's fees as the U.S. Government does when it is involved in litigation under the Equal Access to Justice Act. So those are solvable problems.

Senator MORAN. I take that as encouragement as we have tried to solve them for about 2 years now. Let me ask Mr. Reed before I need to go. You know Colorado—Virginia, Colorado, they have enacted data privacy legislation and we call that up concerned about a patchwork of laws. We have been warned previously steadily about a reality of increasing pressure on Congress as more states adopt those State laws.

What about the nature of doing business on the Internet makes it untenable for businesses to operate in an environment with different states, where different States have different privacy standards?

Mr. REED. I think I caught most of that, but the answer, Senator, would be—well, Virginia and Colorado bills were both excellent bills, but ideally a Federal preemption would be better for some simple reasons. Even within the confines of those two plus California plus a few other states, there are terms and specific differences between there. As you know, in breach was a classic example. There are 47 different breach bills in some states. If you got a request from law enforcement, you needed to wait to tell the customer that it happened. In another state, you had a situation where you needed to tell the customer immediately and then inform law enforcement. For small businesses, that kind of compliance regime, the same thing in privacy of how do I see consent?

For example, if one state says the size of your belt is biometrics, then I need to get your consent if I want to know your belt or shoe size, because I am an app that helps you buy shoes. In another state, biometrics may be defined as a retinal scan or a fingerprint. So from a small business perspective, it is not just the language of the bills, but it is the way the definitions are done, the way the report language in each state is done.

And that raises our compliance costs and our lawyer costs. And it is a really solvable problem because our goal is to get the customer to—to give them a product they want and to earn their trust.

Senator MORAN. Mr. Reed, thank you. Thank you, Chairman.

The CHAIRWOMAN. Thank you. Thank you so much. Senator Markey, I don't know if you are ready to go now, but I want to thank you for your indulgence there with our colleagues and also thank you for your leadership on COPPA and your work back there, get-

ting your staff more up to speed on what you are going to do—as opposed to the other way around.

[Laughter.]

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

Senator MARKEY. Thank you. Thank you, Madam Chair, very much. Thanks to our expert panel. Yes, we are in a crisis. Children are being targeted as we sit here right now by hundreds of companies that just don't care about kids, don't care about their privacy. And that should be the one thing we all agree upon, that children should not be allowed to be preyed upon. Here are the numbers. It is frightening. Children's time on their devices has doubled over the last year, doubled over the last year.

A study of kids Internet use found 144 percent increase in the number of messages children sent and received online in 2020 versus 2019—one year. Today, 70 percent of parents estimate that their children spend at least 4 hours with screens every single day. So to each of you, please, yes or no.

If we can't pass a bill which protects adults' privacy, should we ensure that we pass a bill that protects children's privacy in this Congress? Yes or no, Mr. Vladeck?

Mr. VLADECK. Yes.

Ms. OHLHAUSEN. Children's privacy is very important, and I often point to COPPA as a very positive——

Senator MARKEY. Yes or no, should we increase the protection?

Ms. OHLHAUSEN. Well, I haven't seen the bill, so I don't know.

Senator SCOTT. I am not asking you for a bill. Should we protect children? If we can't protect adults, should we at least get children done in this Congress?

Ms. OHLHAUSEN. Yes.

Senator MARKEY. OK. Yes. Thank you. Mr. Reed?

Mr. REED. Sure.

Senator MARKEY. OK, good. Thank you. And——

Mr. SOLTANI. Yes.

Senator MARKEY.—Mr. Soltani. OK, thank you so much. Now the reality is—thank you, Mr. Vladeck. Going back to 1998, 1999. Yes, I put to limit it to children under 13, but that wasn't my goal. It was to have it under 16 but the industry said no back then. You didn't have to be a genius to figure out a business model to exploit children, because historically industries had done it on television with television advertising, which is why we need children television advertising. So, you know, I was just blocked back in 1998, 1999 from raising it up to 16. So it is not a new issue.

It is like all of a sudden, oh my god, who would have ever thought that people would exploit children with technology that have been going on, you know, for many, many decades up to that point. And that is why Senator Cassidy and I have introduced Children and Teens Online Privacy Protection Act to increase the protections up to age 16. Mr. Soltani, can you briefly discuss the importance of banning targeted ads to children?

Mr. SOLTANI. Yes, absolutely. Thanks for the question. So I think there is a key issue that COPPA doesn't really solve for data abuses once the consent has been given. And ads that are inher-

ently manipulative, kids have a harder time detecting or knowing particularly when they are hyper targeted and personalized, using their kid's name or age or using their friend's likeness.

More importantly, the harms of collection for kids are also higher. Kids have a limited ability to detect misuse or abuse of their data, identity theft, et cetera. So absolutely, I think considering a ban on OBA and targeting for kids is incredibly important. I think it would essentially deal with not just the privacy issues, but some of the other addiction and manipulation issues, dark patterns, etcetera, the kids are much more susceptible to.

Senator MARKEY. Yes, and—thank you, Mr. Soltani. And that kind of targeting is banned in the bill, which Senator Cassidy and I have introduced. And again, I just think we have to put these laws on the books. And Mr. Vladeck, in terms of the with what the UK has done in implementing its age appropriate design code, a law to protect young people online—we are behind the UK right now. So can you talk a little bit about how what the UK is doing anticipates what we should do in the United States to upgrade the protections for children?

Mr. VLADECK. I am sorry, I am not up to date on what the UK is doing.

Senator MARKEY. You are not? Mr. Soltani, are you up to speed on that?

Mr. SOLTANI. I am not an expert on it. I do agree that the code requires that app developers and software developers maintain certain standards. And I do agree that this Congress should absolutely consider or provide the FTC rulemaking authority to provide some of those.

Senator MARKEY. And the reason I mentions it, Mr. Vladeck, is that you mentioned constructive knowledge in your statement, and that is pretty much what the UK has done in terms of the protection offered to children.

Mr. VLADECK. Right, and from enforcement standpoint, that is the key question.

Senator MARKEY. Thank you—that we need to protect. We need to assume constructive knowledge in terms of the activities.

Mr. VLADECK. Yes, that is correct. That is the key change in the statute.

Senator MARKEY. Yes, thank you. And again, we need to change the law so that if we are successful in putting the funding in to the Federal Trade Commission, that they have a law under which they can act in order to say to companies that are exploiting children, no, we are coming after you. And so it is all tied together. And if we put in the money for a privacy bureau at the Federal Trade Commission, but we don't change the law, so the kids are protected, then we really haven't finished the job. Thank you, Madam Chair.

The CHAIRWOMAN. Thank you. Senator Thune, I believe, is joining us remotely.

**STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA**

Senator THUNE. Thank you, Madam Chair, and thanks for today's hearing. I believe that enacting comprehensive privacy legis-

lation should be a top priority of this committee. And since we began privacy conversations in the aftermath of the Cambridge Analytica scandal, when I was—served as Chairman of the Committee, I have stated that there is no question we need a Federal law to protect consumers privacy. And I do not believe we should relinquish all responsibility by simply increasing our Federal bureaucracy, by putting a significant amount of funding at the FTC, I should say. So it is my hope that we can work together in a bipartisan fashion to establish uniform national policy. I push for more transparency about the algorithms used by big tech companies to analyze consumer data and make predictions intended to influence consumer behavior.

Many consumers are unaware that much of the content that they see on the Internet platforms is determined by sophisticated algorithms that draw on data about each consumer's online activity. Billions of people are being fed content on Internet platforms as basically selected for them by opaque algorithms designed to keep consumers engaged on the platform. The powerful artificial intelligence behind these platforms creates a unique universe of information for each user, phenomenon that is often referred to as the filter bubble.

Earlier this month, the *Wall Street Journal* revealed that Facebook altered its opaque algorithm after seeing a decline in user engagement. They change in the algorithm that was intended to optimize user engagement resulted in more divisive, manipulative content being pushed to users. This troubling report is exactly why I introduced the Filter Bubble Transparency Act, and I am proud to have strong bipartisan support for this bill with Senators Blumenthal, Blackburn, Moran, Schatz, Warner, Collins, and Klobuchar as co-sponsors.

Our legislation would give consumers more transparency about how algorithms are used to select content that they see online. And it would give consumers the option to engage with Internet platforms without being manipulated by opaque algorithms. So very quickly, I don't have a lot of time left, a couple of questions here. This is for each of you. Are Internet platforms doing enough to provide users with the transparency they deserve to make informed decisions about how they interact with the platform's services, yes or no?

The CHAIRWOMAN. Who wants to start—

Mr. REED. Well, I will start and say no, but part of the problem is we are taking it from a compliance perspective. Merely adding another page to a terms of service or a click through doesn't actually achieve knowledge and doesn't actually allow the user to understand what is going on. So we have got to find a way to solve the problem that just doesn't add another page to a compliance document.

Senator THUNE. OK. Yes or no, other members of the panel.

Ms. OHLHAUSEN. So I agree that legislation could be very beneficial to provide additional transparency to consumers.

Mr. VLADECK. There is really no transparency to consumers. So, yes, we do need legislation to enable consumers to have a better sense of how decisions are being made.

Mr. SOLTANI. Senator, no, I don't think enough is being done, and often the companies don't themselves know how their systems work, and that is why it is important not just to have transparency by the companies, but also have resources at the Federal Trade Commission that can verify those claims and those representations.

Right now, to my knowledge, while the FTC has great staff and great technologists, there is not a single AI or algorithmic transparency expert at the Commission that can verify the claims that companies make. So to your question of big—Government, I do think it is important that they have expertise and resources to support the great legislation you are proposing.

Senator THUNE. And very quickly, do you agree that consumers ought to have the ability to use Internet platforms like Facebook, Twitter, and YouTube without being manipulated by algorithms designed to keep them engaged on the platforms?

Mr. SOLTANI. Is that to me?

Senator THUNE. Anybody. Just yes or no? Yes, I mean, it is a pretty straightforward question.

Mr. SOLTANI. So I will jump in. So I—Go ahead, David.

Mr. VLADECK. No, you go ahead, Ashkan. Sorry.

Mr. SOLTANI. Sorry. I do think that having the ability to at least understand how the system works and there is you know, there is algorithmic targeting based on general machine learning of the population and based on your personal data. I think the latter, or I'm sorry, the former will be harder to limit but you can provide transparency to it. The latter, targeting and manipulation based on information about you, I think clearly you should have the ability to disable that hyper personalization and filter bubble activity.

Senator THUNE. Alright. Very quickly, do you all believe that we ought to need—that we need a national standard that says the same rules across the entire United States to ensure consumer protection?

Mr. REED. Yes, we need Federal preemptive privacy bill.

Ms. OHLHAUSEN. Yes, I agree,

Mr. VLADECK. I too, I agree as well.

Mr. SOLTANI. I don't think the standard needs to essentially preempt the states, but allow experimentation in the states, particularly because there is a bunch of different approaches and issues here. So as long as the standard can allow states to go further, then, sure.

Senator THUNE. Thank you all. Thank you, Madam Chair.

The CHAIRWOMAN. Thank you. Senator Hickenlooper.

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

Senator HICKENLOOPER. Yes, thank you. And thank you all for putting in the time and your public service. Really is illuminating. I am a former small business owner, as has been discussed already. I think regulations had to be carefully tailored to ensure fairness in regulation, but also appropriate oversight.

I think you are all aware of the Colorado Privacy Act, applies to businesses with at least 100,000 data records or a business with 25,000 data records held and deriving some revenue from sale of data. It is different than other State laws in terms of applying rev-

enue—other laws applying revenue threshold as a percentage. So Mr. Vladeck, would applying a privacy law to any business earning any revenue from the sale of personal data, does that efficiently promote broad compliance to require consumer protections? And why or why not?

Mr. VLADECK. Well, there may be some constitutional issues with Congress under the Commerce Clause regulating really small businesses. But, you know, my own view is that at some point, State laws are going to fall, and not because of Congress necessarily, but because of the dormant Commerce Clause. And, you know, you are going to get a collision of State laws, which is why at some point Congress is going to need to pass a comprehensive privacy statute.

But, you know, I worry that carve outs for small businesses without some subtlety to it would allow companies that can be incredibly disruptive on the Internet, tiny companies to evade regulation. When—during my tenure as Bureau Chief at the FTC of Bureau of Consumer Protection, we went after some small companies that created massive harm. So—

Senator HICKENLOOPER. Can you give me an example?

Mr. VLADECK. Sure. So Frost Wire was about to send out an app, a file sharing app with a default that would—hard to disable, that would have required—that would have permitted or encourage file sharing. Designer Wear designed an app that allowed remote activation of a computer's camera, you know, and so—you know, and that is—you know, that app was installed in millions of computers that were then rented and then sold to consumers and the clerks, you know, in the rental office did often just simply turn on the computer and see what was going on in your house.

So, you know, there are small companies that can cause enormous harm. And so I am sympathetic to the need to promote an innovation with small incubators that need to be protected. But there also has to be a balance because some of the small companies have caused great harm.

Senator HICKENLOOPER. Those are sufficiently gruesome that I am almost sorry I asked.

Mr. SOLTANI. And Senator, if I may—it I may jump in. Additionally, it is no longer the small developer in their bedroom. Oftentimes these are VC supported or, you know, angel supported companies. When I was at the FTC, we did kind of a road show where we met and interviewed a number of VCs in the investment community. And often they do not absolutely invest in security or privacy from the start. They don't look—it is actually what they consider a waste of money. And as Professor Vladeck mentioned, oftentimes small companies can have a real significant harm to consumers and completely obliterate their requirement to do any investment in security or privacy and cause great harm.

So I think it is—it needs a bit of nuance, as you consider that carve out.

Senator HICKENLOOPER. No, absolutely. I appreciate that. Mr. Reed, again, the Colorado Privacy Act was passed in July of 2021 and again allows a narrow and temporary right to cure on private deficiencies. But this right of cure defaults after 2 years. And I know we have discussed about this a little bit, but I thought more specifically though, how could a narrow and temporary cure period

help small businesses, let's say, well intentioned small businesses and startups to adapt to new regulations for privacy?

Mr. REED. Right. And as you know, we actively supported passage of the Colorado bill and we are hopeful that it and some like it serve as a model that we can move forward on. So you asked for how does it—how does it work, right. So, again, for a legitimate business that isn't trying to manipulate or spy on people through rental computers, all of those things are exactly the kind of harm that the FTC should be going after.

If you are a legitimate business that is trying to acquire customers or deal with people, then the right to cure allows you to fix something that either, a, you didn't communicate clearly through your terms of service or, b, that didn't match the expectations of customers. And so the period of cure is really critical because if you failed in one of those two things, your primary job is to solve it because you want to stay in business.

So absolutely, that is how we see a narrow period of cure working. And again, that doesn't prohibit the ability of the FTC or State AGs to go after truly bad actors like the one that Professor Vladeck raised earlier.

Senator HICKENLOOPER. And thank you very much, Madam Chair. Thank you.

The CHAIRWOMAN. Thank you. Senator Lummis.

**STATEMENT OF HON. CYNTHIA LUMMIS,
U.S. SENATOR FROM WYOMING**

Senator LUMMIS. Thank you, Madam Chairman. We all know that large technology platforms have been given unfettered access to collect data on the most sensitive areas of our lives, often without our knowledge or consent. This data is then repackaged and sold to the highest bidder or used to fuel algorithms that target us with overly invasive advertising.

So I applaud the Committee. I applaud you, Madam Chairman. It is long past time that Congress shine a light on these unsupervised practices. I am concerned, however, that despite our best efforts, Congress may be outmaneuvered by these tech platforms. It is like a magician who uses misdirection to distract his audience. These companies have already used practices that bypass the guardrails that Congress intends to put up, and more are on the way.

I had an Op-ed published yesterday that underlined some of these activities, and I ask that it be included in the record.

The CHAIRWOMAN. Without objection.

[The information referred to follows:]

THE BIPARTISAN REASON CONGRESS SHOULD REGULATE BIG TECH

BY SEN. CYNTHIA LUMMIS (R-WYO.), OPINION CONTRIBUTOR—09/27/21 7:00 PM ET



In Wyoming, privacy is a way of life. We are the smallest state by population, but among the largest in physical size. Privacy is baked into our lifestyles since many in the Cowboy State live miles from their nearest neighbor.

The Internet has aided our relatively isolated way of life. It has enabled us to more easily keep in touch with relatives, conduct business, and entertain ourselves. But it has not changed that very Wyoming desire for personal privacy.

What concerns me, is that some of the companies serving as the chief enablers of our connected lifestyles and Internet access are undermining our privacy rights. And they are doing so in broad daylight, but going mostly undetected.

Let's start with the latest example: Apple. Apple recently announced a welcomed delay to its program *that would have begun scanning iPhones for images of child abuse*. Now, let's start with the obvious: as a mother and grandmother, I abhor child abuse. But, Americans must take threats to their civil liberties seriously. In fact, reports claim that some of Apple's own employees were protesting against the adoption of this new policy, fearing that it could be exploited by bad actors. Thankfully, your voices were heard, but we must remain vigilant.

It was only a few years ago that Apple fought the U.S. government tooth and nail when the FBI pressured them to unlock a terrorist's iPhone. Even by considering this proposal, it seems those days are long gone. And when the government pressures private companies to invade your privacy, every American should be concerned. The reason is simple: we oppose the creation of a surveillance state. Once built, who's left to stop this technology *from being repurposed to surveil other intimate parts of our lives, or to monitor political speech, as they already do in China or Russia?*

And what about Facebook? For several years, Facebook has *created "shadow profiles" of non-Facebook users* for its own ad services. The data it collects on each person allows Facebook to build a comprehensive profile of a person who is largely unaware that it is happening, and is unable to control it. This means if you've never had a Facebook profile, but your friends do, then Facebook uses information posted about you and compiles it into a "shadow profile." Unlike users, you never gave Facebook any information about yourself. Frankly, Facebook doesn't care. This raises all kinds of red flags.

Up next is Google's Federated Learning of Cohorts, or FLoC. FLoC is Google's replacement for third-party trackers. Rather than individualized ads based on your browsing history, *Google uses FLoC to place users into an anonymous cohort* with other users based on web searches and other behavior. This is troublesome because, for example, a user might be placed into a mental health related cohort for googling

about substance abuse treatments. Additionally, this means that your browsing history is still being tracked. It is entirely possible that, despite Google's efforts, it will be easier for companies down the road to reverse engineer, or "fingerprint," exactly who a user is based on these cohorts.

Finally, Amazon. Amazon recently received approval from the FCC to use *radar technology to monitor your sleep habits* and "motion in a three-dimensional space." This technology has not been implemented yet, but Amazon is clearly gearing up for deployment. Certain Amazon hardware like Alexa has already been shown to continuously "listen" to pretty much every conversation within its radius, but this 3-D monitoring is a realm of science fiction that we have never before realized. If we can't enjoy privacy in our own bedroom, then what is left?

This is not a comprehensive list, just some of the most egregious examples from the largest tech companies. These are also not instances of political policing or preference. The right to privacy is a bipartisan issue.

Such actions are incredibly alarming and sobering. However, ultimate blame belongs with Congress, for not taking action.

As a freshman senator, I have been mostly sitting on the sidelines of the big tech debate, monitoring the issue and learning. Unfortunately, our tech companies are not quietly waiting for us to come up with confines for them. They are innovating and pushing boundaries because we have not set any.

It's time to act, and I look forward to learning more at this week's Senate Commerce Committee hearings on protecting consumer privacy. In the privacy-loving Cowboy State, we know that fences make good neighbors. It's time Congress puts up some fences around big tech.

Senator Cynthia Lummis is the junior senator from Wyoming.

Senator LUMMIS. We all must gain a better understanding about the types of data collection activities that the large platforms are utilizing. We must know who has our data? What types of data do they have? When are they collecting our information? Where is it being sold? And how is it being used? We can't hope to craft a strong bipartisan, consumer oriented framework for data privacy without that information.

So I am hoping this hearing is moving us closer to enacting that framework. And now I have a question for any of the witnesses that feels you want to weigh in on this. So my first question is on specific data collection practices. I am concerned that these don't fall within the scope of the California CPA or the European Union's GDPR or the proposed bills here. An example is the Facebook pixel. The Facebook pixel is used by numerous websites to identify unregistered visitors to that site.

Since the pixel loads with the webpage, consumers have no ability to opt in or opt out. This practice allows Facebook to determine that person's identity and record specific data about their web activity. This enables Facebook to collect data on nearly every consumer and target them with high precision advertising. Does this panel feel that this type of data collection would be covered under any of these laws?

Mr. SOLTANI. I am happy to start.

The CHAIRWOMAN. Yes, that is a good idea. Mr. Soltani.

Mr. SOLTANI. So, I am quite aware of the kind of surreptitious tracking you describe and I won't speak about GDPR, but under CCPA and CPRA, the essentially third party tracking, where the transfer of data, for example, by the first party to Facebook would be constituted—would constitute a sale under the CCPA and the CPRA, and consumers are allowed to opt out of that transfer by indicating, for example, on *The New York Times* that they don't want their information sent or sold to Facebook.

Importantly, the CCPA and CPRA also provide consumers rather than having to opt out on every website they click on, or they visit, they can set a setting in their browser called the Global Privacy Control, which essentially sends that signal and indicates their opt-out preferences to every website they visit.

So, for example, if I have and today, if I go to *The New York Times* or *The Washington Post* using a browser that supports this protocol, I am automatically opted out of the sale of my personal information to those third parties and the California AG is able to enforce when that transfer does occur.

Senator LUMMIS. So could that also apply to the example I used like this Facebook pixel, which loads with the webpage?

Mr. SOLTANI. Exactly. So that is precisely the type of transfer it is intended to curb. Essentially, *The New York Times* is making available consumers data to Facebook as a sale. And so when you opt-out of a sale, you essentially have—*The New York Times* would restrict that data transfer to Facebook.

There are some caveats with regards to whether Facebook would operate under the context of the service provider and therefore not use users' data for their own benefit, but only for, for example, measurement for the benefit of *New York Times*. And that is in the AG's rulemaking. But effectively, this surreptitious silent pixel based, third party pixel based tracking is intentionally one of the key aspects of the law.

Senator LUMMIS. Are any of you aware of other data collection practices that similarly bypass, at least opt-in requirements of existing privacy laws?

Mr. SOLTANI. Happy to jump in on that one. Go ahead.

Mr. REED. Yes, no, go ahead.

Mr. SOLTANI. So, absolutely. So one of the biggest gaps, I think, in privacy law today, including with CCPA and CPRA, are a collection from websites that consumers don't interact with. So not just when I interact with *The New York Times*' best seller, share my data with Facebook, but really the myriad of data brokers that collect my information either from across the web, either from me to public records or private records, where they purchase it from companies that I have essentially—I am not aware of, or even when companies will, for example, capture data that appears in public records, as I said.

And so that—curbing that behavior is incredibly difficult because consumers don't have a direct relationship with the third-party data brokers that are selling their information. And no framework really is able to curb that today. Consumers can today go under the California law and opt-out of each data broker, but they have to take some action or employ an authorized agent, a company, a service that will go and delete or opt-out their data for them, right. And this is a huge gap, right.

So a good example is I don't know if you have Full Contact. They are an e-mail provider that, for example, in order to use a service for free, I give that provider access to all of my e-mails, which includes the e-mails I have sent to you, Senator. And therefore, they are able to get your contact information, your phone number, all that information from those e-mails and then further sell or share

that information. That is something we have a very difficult time really addressing today.

Senator LUMMIS. Thank you for your response. I would love to—yes, sir.

Mr. REED. Just very quickly, there is one aspect of this that we keep coming back to. And part of it is you asked a question about consent to. Another former FTC alum, Professor Lorrie Cranor, who is also the CTO at the FTC. She has done significant research about, do people understand what they are consenting to in the first place?

And so as we are talking about all of these consent mechanisms, the thing to really remember is what are we trying to achieve? What is the behavior change? What is the outcome we are trying to achieve? So when we asked the question about, did they did they consent? Did they know what they consented to?

The CHAIRWOMAN. Thank you. Senator Peters. Although I think, Senator Lummis, you just made the point of why we need more technologists at the agency, because the only person who could answer the first question was Mr. Ashkan Soltani. So anyway, these things aren't mysterious. They aren't that mysterious. You just need people who understand the technology to basically help inform the lawyers and the other policymakers about some of the—thank you, though. Senator Peters.

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

Senator PETERS. Thank you, Madam Chair, and thank you for this hearing. And I want to pick up on some of the answers to the questions by Senator Lummis and actually a bill that the two of us have introduced related to data brokers. And I had asked additional questions of Mr. Soltani. But when I think about data brokers and why we have introduced this bill as an example, in 2019, a data broker tried to sell the names, the addresses, the high schools, and the hobbies of 1.2 million children. And this was uncovered through a violation of Vermont's recently enacted law.

And those State law—and through State law was discovered that another company called Amerilist was selling the name, home address, age, religion, education level, and income of 5,000 people for \$150. And so that is why Senator Lummis and I have joined together trying to seek more transparency in this. We have introduced the Data Broker List Act to ensure that data broker companies actually register with the FTC. The bill would require companies to provide the agency with the types of information the company has collected and an explanation for the purpose of why that data is collected.

First question for you, Mr. Reed, in this. In your testimony, you noted that 89 percent of mobile devices have denied data features to apps they didn't trust, and over half of the users have deleted apps due to privacy concerns. So I am interested in hearing your suggestions on how we improve and expand the Vermont law that I have already mentioned had an impact in identifying abuse, as well as California data broker laws at the Federal level. Particularly how to ensure that data brokers are transparent with this information. What suggestions do you have for us?

Mr. REED. So first of all, I think that looking at both Colorado and Virginia's recently passed bills are also incredibly helpful on this. But one of the things to be aware of is something that Mr. Soltani mentioned. Right now in California you can go to the website, and you can see the list of data brokers. You can click to them. How many consumers actually go to the Government page and wallow through their poorly written HTML code to find the click link to go to figure out who their—what the data brokers are and what they have on them.

So part of it is not merely finding a way for the data brokers to say, yes, you know, find me here. But to actually engage with the consumer at the point of which their data is collected and make sure that the party who is collecting that information is responsible or at least is communicating clearly, and I don't mean page 37 of a terms of service, about what they are doing, who they are providing it to.

Because you are talking about the data brokers, but the data brokers have to get that data from somewhere. And that is the point of inflection in which the consumer has the most impact. So while I think it is good to have a list of data brokers and I think it is good to have transparency, let's start at the point of impact. And that means my members, they have to communicate clearly to user. Here is what I want. Here is what I am going to do with it.

Here is what I am not going to do with it. And I think you will enjoy my product. And if they can't say that, then they shouldn't be on a platform.

Senator PETERS. Some smaller data brokers have suggested that they should be completely exempt from reporting and disclosure requirements. They are a small business and that—

Mr. REED. Absolutely not.

Senator PETERS. You have already—the question is, should Congress consider FTC exemptions for data brokers? Should we treat them like we do your average small business down the street?

Mr. REED. No, because they aren't the small business down the street and they are not the point of inflection, right. They are not the point at which you, the consumer, engaged with the activity that provided your data. So they are opaque to most users. And so, no, I don't think that they should be exempt completely because they are no different than the local small business or the bike store.

Senator PETERS. Absolutely. And one final question, Mr. Reed. I am a founding member of the Senate's Artificial Intelligence Caucus, and I would like to hear from you about how companies are using AI to preserve privacy. And where do you see some challenges and what role do you think the FTC should play in ensuring that we are dealing with some of the challenges of AI while not discouraging innovation?

Mr. REED. Well, I have to put a plug in for our white paper on good machine learning practices, which we have developed. But you are asking a really important question. AI can help to preserve privacy. It can do so by making sure that you strip out data that is personally identifiable before you actually do the learning. The place that has created the most, and I am looking at time, the most difficulty in understanding how we move forward is in health care.

I am honored to serve on Federal Advisory Committee for HHS on some issues around education and outreach. One of the biggest problems in the AI space is, I don't need to know if you like blue interiors on cars, right? I don't need to know that Senator Peters likes blue interiors. I just need to know that a large group of people like blue interiors and so I make a marketing decision. Now, if I need to know what medication works best for a group of people with several comorbidities, then I need detailed information. And that means I need your private information, your most private information to know what medication works, what treatment regime work best, what are the things that I should warn you about in advance. Digital retinopathy.

There is so many places where knowing more about you allows me to keep you healthy and safety earlier in the process through the physician. So when it comes to AI, the questions that are to ask, is it necessary to have that extra data to provide some very specific value, especially in health care, to the customer—to the person—I keep talking customers. They are people—to the people.

If it is something where I just need to know, hey, you like blue interiors and 10,000 other people like blue interiors. Oh, but they also like silver trim. Great. I need to remove the identifiable information on you when I am training that engine to develop what I am going to do for my marketing material. So I think there is this split. Sometimes we need it to provide a need and a good, sometimes we don't.

And in that way AI can actually be useful to strip out the parts that we should be—we should be leaving on the sidelines.

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

The CHAIRWOMAN. Thank you. Senator Lee.

**STATEMENT OF HON. MIKE LEE,
U.S. SENATOR FROM UTAH**

Senator LEE. Thank you, Madam Chair. And Ms. Ohlhausen, I would like to start with you, if that is all right. Earlier this year, the FTC took some steps to remove some rulemaking barriers to their authority under Section 18 of the Federal Trade Commission Act. They wanted to make it easier for the Commission to engage in rulemaking.

Now, these procedural requirements that they are trying to get around were put in place in the 1970s after the Federal Trade Commission had gone on something of a rulemaking binge. So Congress put in place restrictions on that power so they would be less inclined to do it again. So I find it a little bit surprising, shocking, in fact, to see these rather blatant, bold efforts by the Commission to seize rulemaking power against manifested Congressional opposition and statutory impediments put in place designed to discourage that.

Now, I am skeptical that Congress should even grant the Federal Trade Commission broad rulemaking power, APA universe style rulemaking power, to the Federal Trade Commission. But setting that aside, should Congress even consider granting this rulemaking power with the current trajectory being undertaken by the Federal Trade Commission to flaunt, rather cavalierly disregard restrictions on the rulemaking power that it is already in place?

Ms. OHLHAUSEN. So, Senator, you know, the FTC definitely has a checkered history with rulemaking, and that is why the Magnuson-Moss Act and the Federal Trade Commission Improvement Act got enacted by Congress to put particular guardrails in place. So the more clarity Congress can give to what it wants the FTC to do, I think that comes—you know, that works much better.

So when you think about the Children's Online Privacy Protection Act where Congress set the boundaries, Congress set the age limit, and then gave the FTC the authority to update what is personal information based on how technology changed, I think that was a really good model.

Senator LEE. Yes. No, clarity certainly helps. And I am sure you can understand my frustration and my reluctance to give them anything in light of the fact that they haven't complied with existing restrictions and seem to be looking for ways to get around them. Now, as we consider what else we might do with the FTC and as we take into account the rulemaking abuse over the decades, I want to analyze that against the current backdrop of the proposal to create a new FTC privacy bureau.

My understanding is that the FTC's Fiscal Year 2022 budget request amounted to \$389 million. The House's reconciliation bill, the \$3.5 trillion reconciliation bill proposes including an additional billion dollars on top of that to give to the FTC. And the intended purpose for that is, and I am going to read the entirety of the legislative text that deals with this issue. Here it is. It is to, "create and operate a bureau, including by hiring and retaining technologists, user experience designers, and other experts, as the Commission considers appropriate to accomplish the work of the Commission related to unfair or deceptive acts or practices related—relating to privacy, data security, identity theft, data abuses, and related matters."

So, Commissioner Ohlhausen, setting aside for a minute whether we have \$1 billion to spend on this right now, which I don't believe we do, but setting aside that issue for a moment, how would this—what kind of conflict might this create within the FTC? Conflict, for example, with the Bureau of Consumer Protection. And how is that language—you referred a moment ago to the need to give them clear directives. How does this comport with that or does it?

Ms. OHLHAUSEN. So I think it is important to pair both additional resources and additional statutory guidance and clarity to the FTC for its privacy enforcement. We have talked a lot about privacy. I think that, you know, is a useful thing. But the FTC does a lot of other important enforcement in areas, you know, as varied as unsafe products, you know, deceptive advertising, credit issues. I mean, the list kind of goes on and on. So I do think that, you know, we don't want to sort of disregard the other important things that the FTC does. But I think those—the resources and the statutory clarity need to be paired.

Senator LEE. OK, I see my time has expired and so I am going to move on. I wanted to ask you a little bit more detail about the nature of the data privacy harm but i will do that in writing. Thank you, Madam Chair.

The CHAIRWOMAN. Senator Rosen is next.

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

Senator ROSEN. Thank you, Chair Cantwell and, of course, Ranking Member Wicker for holding the hearing today, it is so important. I want to thank all the witnesses. The testimony has been very good. I appreciate everything that you are working on. And I want to talk a little bit about health data privacy, because I am a member of both this Commerce committee and the Health committee. And so I have an opportunity to see up close the intersection between technology and health care. Wearable technology has been at the forefront of the Internet of Things, and it offers greater insights into our health every day, how we can improve it, monitor it, et cetera, et cetera.

You know, last year alone, there were more than 90,000 health apps that were released, including apps for fertility, medication, even to sleep better. So despite these exciting developments, I am concerned with the ability of companies to use that data that they have accumulated from the health apps and the wearables to draw inferences about individuals and groups.

And so these assumptions are that we as individuals may not have the opportunity to verify, but they can nonetheless significantly impact our lives, sometimes even leading to profiling or discrimination. That is why Senator Cassidy, and I reintroduced the bipartisan Smartwatch Act, which extends existing health care privacy protections under HIPPA to personal health data collected by apps and by wearables, preventing this data from being sold or used commercially without the consumer's consent.

So Ms. Ohlhausen, can you discuss some of the challenges with protecting consumer health data that we are seeing and some of the examples of best practices for protecting this data that might not currently—might not currently be under HIPPA? Where do we need to expand?

Ms. OHLHAUSEN. Yes, Senator. It is—it became apparent as health apps and other online sort of uses for health data were not covered by HIPPA, so they didn't necessarily have those HIPPA-like protections in place.

So I think the FTC has actually been fairly vigilant about making sure that the collection and use and sharing of sensitive personal data, which health data would be considered that, is done with the knowledge and consent of consumers, and that it is not done in a way that harms consumers. And certainly discrimination would be, you know, one of the prohibited harms for that. So I think that the FTC has been active in that space, and I hope it will continue to be.

Senator ROSEN. Thank you. I appreciate that. But you know, we need to address some of the challenges. The Federal Trade Commission has issued a policy statement affirming that health apps and connected devices that collect or use consumers' health information must comply with the health breach notification rule. This rule requires that apps and devices notify consumers when their information is breached.

So, Mr. Soltani, do you believe the FTC's policy statement goes far enough to protect consumers' health data? And if not, what rec-

ommendations might you have for us here in the Senate regarding these policies to strengthen the protection of consumer health data?

Mr. SOLTANI. That is a great question. Thank you. Absolutely, I think we would need to expand those definitions to not only include the kind of narrow definitions of health data, but also some of the related health related data and that my co-panelists mentioned, particularly when thinking about things like AI and inferences and machine learning, where oftentimes the data is inferences that the consumer didn't necessarily provide, but that were made by the software system about the consumer.

And so we want to make sure that the agency has adequate ability to identify those problems and also create rules and standards for safeguarding that information.

Senator ROSEN. Thank you. I want to quickly kind of add on to that because we have very vulnerable populations, particularly our visually impaired and our hearing impaired populations. So these technology advancements, they really can help people locate in places and mobility impairment. We have all kinds of things in that space. And so these kinds of populations are vulnerable populations that really rely on this adaptive technology to—for their day to day lives.

So this technology is not a choice where it might be for some other app. So, again, Mr. Soltani, how do you think we can add to our privacy laws to protect our medically vulnerable or vulnerable populations, such as a hearing impaired, mobility impaired, or visually impaired?

Mr. SOLTANI. Absolutely. I think those considerations, again, have to be made. When you think about, it is not just vulnerable populations, although I think they are incredibly important, but even today, due to COVID and due to the way we are living our lives, we are forced to use and adopt technologies because our doctors will push them on us, right.

And so we need to essentially make sure that those realities of the fact that we don't often have choice and are required to provide consent, even though we may not want to, creates a lot of problems with regards to the data collection and use. So the ability to, for example, opt-out of any secondary use, restrict the data to be—or require the data to be deleted after was immediately used and require companies to store it securely for the time they do have it, I think are going to be critical both to any future legislation, but also guidance to the FTC.

Senator ROSEN. Thank you. I think those are—excuse me, some great suggestions. And I look forward to us being able to work with you to find ways to implement those. Thank you, Madam Chair.

The CHAIRWOMAN. Which one of you showed—Senator Luján, Senator Warnock, which one of you—I thought—anyways, whichever one of you is next. Senator Warnock, thank you.

**STATEMENT OF HON. RAPHAEL WARNOCK,
U.S. SENATOR FROM GEORGIA**

Senator WARNOCK. Thank you so very much, Madam Chair. Privacy violations affect all of us and so we are grateful for this hearing. While all of us are affected by privacy violations, those harms can fall unequally across communities. We have seen historically

how marginalized communities or historically marginalized communities particularly suffer from tech companies' unchecked data collection and use.

In 2019, HUD actually sued Facebook for housing discrimination, because its algorithms targeted housing ads based on sensitive information, such as where people lived, whether they were a mom, if they were—or their religion. We have also heard reports of how platforms allow businesses to discriminate on who actually sees certain job advertisements so that the technology is re-inscribing in new ways old problems of discrimination and marginalization.

Showing ads to young men and not to women or older Americans. Professor Vladeck, how can the FTC use its investigation and enforcement powers to hold tech companies accountable when they enable and further deepen patterns of discrimination?

Mr. VLADECK. That is a great question and I think your description of the problem is spot on. The FTC has the authority to push and to force companies to not engage in biased activity online. And that—you know, those problems would be sort of under the unfairness jurisdiction of the FTC. And the FTC has done some, but probably not enough work in that space. And, you know, my bottom line is, give the FTC more resources and give the FTC a nudge in that direction and it will do its job. But again, the FTC has never had more than a few technologists on staff.

In order to sort of surveil the advertising practices, because that is really where the problem stems from, the FTC would need more resources. We need people online doing the kind of day to day oversight or surveillance that if the FTC were better resourced, the FTC could do.

Senator WARNOCK. I agree that the FTC needs the resources in order to provide this kind of enforcement, which is why 20 civil rights organizations sent a letter last month asking the FTC to create an Office of Civil Rights. Mr. Soltani, what types of structural changes do you think would help the Commission to build expertise and capacity to protect consumer rights in general and marginalized communities in particular?

Mr. SOLTANI. Senator, thank you for the question. Absolutely. I think the effect of these new technology systems on already marginalized communities is immense. Most of the kind of machine learning and AI simply, you know, is machine learning based on what we have historically done in the past. So often they fundamentally re-enforce existing inequities since they just learn from past behavior.

So absolutely, either creating an Office of Civil Rights, an OCR, that works across the agency or as I have suggested, perhaps including that function, making sure that the new bureau that gets created with this funding also has experts and expertise that work across the agency's mission on these issues of discrimination, algorithmic fairness, and bias, I think are incredibly important. Additionally structural changes, to go to the previous Senator's comment, I think rulemaking here, or at least the authority to create rules, the rules of the road are incredibly important.

So I personally have done a lot of this work. I have done worked with *The Wall Street Journal* showing that, you know, companies will charge different prices to consumers based on where they live,

how far they are from a competitor's store, particularly in disadvantaged communities and an area codes. So it is very difficult and hard stuff to do from the outside.

So additional resources would help, but so would essentially guidance to companies that they need to self-test and self-attest, self-verify that their systems do not bias against consumers on areas like, you know, race, gender, age for protected categories like housing, credit, employment, right. And I think companies are in the best position to do this and can provide those attestations to the FTC.

And if the FTC has qualified staff to then review and verify, that would help really move the ball forward, I think.

The CHAIRWOMAN. And just to clarify on that, Ashkan, to the earlier question about transparency and Senator Thune's question to the panel, if you had algorithm transparency, you would then determine whether that algorithm did have bias in it, so.

Mr. SOLTANI. To some degree. Oftentimes, as I said, with machine learning, most of the creators of the system—like in the HUD example, right. So it wasn't that the advertisers themselves or even Facebook intentionally was guiding the algorithm to have disparate impact on who was served certain advertising to who HUD made offers to. It's that the systems to learn.

And so that is kind of difficult to provide just from transparency alone, because it consists of both the algorithms and the underlying data, which is often not available for privacy reasons. So what you would rather do is, in addition to transparency, you want to provide testing and accreditation that the bias doesn't exist on these protected categories.

Senator WARNOCK. Thank you so much. I think with data collection and algorithms and the technology, there is this this sort of perception of objectivity and what we are seeing is a ways in which it further creates increased marginalization, and we have to be vigilant in order to protect that.

The CHAIRWOMAN. Thank you. Thank you, Senator Warnock. Senator Luján.

**STATEMENT OF HON. BEN RAY LUJÁN,
U.S. SENATOR FROM NEW MEXICO**

Senator LUJÁN. Thank you, Chair. I want to thank you and our ranking member for holding the hearing to discuss critical issues involving consumer privacy. As we know today, companies and platforms collect an unprecedented amount of data. And I believe that this committee and Congress should act to protect consumers' data from bad actors. The Commerce Committee has a clear responsibility to ensure that consumers' personal data is only used when the informed consent of consumers is given. Congress must give the FTC sufficient resources to do its job. I support additional funding for the FTC to establish a new privacy bureau.

The Chair fought for such a bureau in the Consumer Online Privacy Rights Act, and I am encouraged to see this critical initiative moving forward. Now, companies have failed to adequately protect data and user privacy. Bad actors have gained access to my constituents' health records, financial information, and Social Security numbers. They have used this data to threaten families' liveli-

hoods, and it has impacted hundreds of thousands of people in New Mexico and millions across America.

This is a real problem, and the problem is only getting worse with every data breach that we learn about. Mr. Soltani, yes or no. Today, does the FTC have the technical expertise to fully protect consumer privacy?

Mr. SOLTANI. Unfortunately, no, Senator.

Senator LUJÁN. Mr. Soltani, yes or no. Would hiring more technologists at the FTC help protect families from data breaches and bad actors?

Mr. SOLTANI. Absolutely, yes. Particularly if you consider technologists broadly, not just folks like myself.

Senator LUJÁN. And Mr. Soltani, you have advocated repeatedly for Congress to invest more resources for technologists at the FTC, so thank you for the work you have done on this topic. In your testimony, you highlighted the importance of having technologists who are empowered to serve the entire agency, and I share your view. That is why I am introducing a bill, the Federal Trade Commission Technologist Act, will establish an office of technologists within the FTC that can work across the Commission to solve these problems.

An office like this would give the privacy bureau the Chair has put forth the tools it needs. It would also provide critical technological expertise in areas like antitrust and competition. Mr. Soltani, do you support my goal of making technologists available across the Commission?

Mr. SOLTANI. Absolutely. I think that is exactly the right move.

Senator LUJÁN. And there are a few other questions I have in that space. I will submit them to the record. The current State of Federal privacy law is a patchwork of requirements varying from industry to industry with many holes. Many of my colleagues today have raised the concerns where HIPPA is a clear example that Federal law was a game changer. HIPPA is a household term now. The legislation and its protection of health information has become fundamental.

For example, if I go to my doctor to get an echocardiogram or genomic testing, the health information they collect from me and my body is protected by HIPPA, but collect the same information from the same place, but with an Apple watch, health app, or consumer biotech, and it is the Wild West. It makes zero sense to me. This month, the FTC announced that they will be increasing enforcement for applications that collect personal health information. But an FTC—but as the FTC Chair noted, this action reflects a more fundamental problem, the commodification of sensitive health information.

As we embark on the task of creating more comprehensive privacy requirements for technology companies, are there any lessons learned from HIPPA and how to effectively protect health data? And I would ask any of the witnesses to come forward.

Mr. REED. Yes, I think—I think one of the things, Senator, that is interesting is, I doubt we have had a more poorly understood law than HIPPA or rather the privacy rule of it. And it actually gets to the core thing that all of the witnesses have been asking for here today, and that is a Federal privacy legislation. As you know, when

HIPPA was passed, the privacy rule was actually done years later, and it was not done by Congress.

And part of the problem is, it is hampered by the fact, and this is why we need Federal privacy legislation—it is hampered by the fact that it is actually triggered by the filing of an electronic insurance claim tied to record portability. And the reason it cannot cover the other material that you asked is because the statute that gave HIPPA its origin story is very closely tied to portability of data.

So a Federal privacy law that actually starts from the premise of we need to protect privacy is the place to start rather than starting from data portability, oh, yes, let's add privacy to it. So it is really the origin story of HIPPA that causes so much of the confusion. And now that is why we are all here today to say, let's have Federal privacy legislation that starts from a discussion of privacy rather than tail on the dog.

Senator LUJÁN. I appreciate that. Well, I am about out of time, so if we could ask you to submit that into the record. I am also going to be submitting a question to the record with my concerns about what the chair pointed out with commodification of sensitive health information. I am very interested in your response there. Last, Chair Cantwell, in the space that was raised a few times by my colleague from Wyoming, Ms. Lummis, specific about Facebook and collecting user information on people that have never agreed to terms of service.

Will also be submitting a follow up to a round of questioning I had with Mr. Zuckerberg when I was a member of the House around how the FTC and Congress can protect the privacy of our constituents who have never signed up for an account or assigned terms of service agreements. Very much appreciate this hearing and look forward to following up.

The CHAIRWOMAN. Thank you and thank you for crystallizing the issue about technologists with the legislation. That will be very helpful. Thank you. Senator Blumenthal.

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

Senator BLUMENTHAL. Thank you, Senator Cantwell, and thank you for having this hearing. There are now some pretty good indications that the Federal Trade Commission is going to have or begin rulemaking on privacy. This development would be very, very welcome. Last week, I wrote to Chair Khan, along with Senators Klobuchar, Markey, and Schatz, and Luján, and four other colleagues urging the FTC to start rulemaking concerning privacy. A coalition of 24 major national civil rights groups, privacy advocates, and consumer groups have joined in the call for that action.

The reason is very simply that Congress has failed to act, in fact, failed abjectly to fulfill its responsibility. Not that the issues are simple or easy, but the FTC is supposed to fill gaps that occur when Congress sometimes fails to do so. I understand that members of the panel have expressed reservations about it. I am not sure I understand the preemption objection. I think the resource issue can be surmounted.

And if Congress were willing to act, of course, that might be everyone's preference, but it is what it is, and in the meantime,

states are also filling the gap. That is the nature of our Federal system, right, laboratories of democracy. But the FTC should start the clock on primary rule—privacy rules. Either Congress acts or the Commission does, and FTC rulemaking at the very least would build a record and provide recommendations to Congress for action. Tomorrow, Senator Blackburn and I are holding a hearing in our subcommittee on Consumer Protection about how platforms like Facebook and Instagram harm the mental health of children and teens, not only invade privacy, but actually knowingly harm children, and in fact, how they have concealed that harm and their knowledge of it.

Over the last two weeks, there have been some pretty chilling revelations about Facebook, including an article just yesterday about its efforts to insert itself into the play dates of children. This would be laughable to a parent who finds it impossible to insert himself or herself into play dates, but it is deathly serious. There are widespread issues with Facebook and kids, including the fact that there are already millions of teens on Instagram, despite restrictions under the Children's Online Privacy Protection Act.

The decision to pause Instagram for Kids is a positive step, but too little, and there should be a permanent pause. I am troubled that the mental health and safety of teens and children are seemingly treated as an afterthought by big tech. These issues of grooming, manipulative advertising, addiction and abuse are rampant.

These practices hurt kids. And what we have all seen from Facebook, I think is deeply disturbing. I know, in Connecticut, outrage is an understatement as to what many moms feel about how their daughters are exposed to the kind of harm that has been depicted so graphically by the whistleblower and the documents that whistleblower revealed to *The Wall Street Journal*.

So I would like to ask Mr. Soltani, in your testimony you talk about how existing enforcement tools don't sufficiently address, and I am quoting, "the psychological harms caused to teens by social media." What additional resources and authorities do you believe the FTC needs to confront this toxic relationship between teens and big tech? And if we have time, I will let others comment on it as well. Mr. Soltani?

Mr. SOLTANI. Thank you for the question, Senator. Absolutely, I think you need both resources and authorities. So as I have said previously, the FTC has limited ability to go after these types of data abuses or data harms under the unfairness authority, particularly because they are often hard to demonstrate. Perhaps, maybe not as much on the issue of kids, but often in any discrimination or any manipulation and dark patterns, it is very hard to get to in fairness. So often the FTC relies on its deception or its deception authority under Section 5.

And so I think having either in legislation or additional authorities for the FTC or at least clarifying that the FTC should issue rules around abuse—data abuse and the use of essentially manipulating dark patterns. Additionally, I think the resources that we are discussing in this hearing today are absolutely critical, right. So right now, if you go to Facebook or Instagram, there are multiple data scientist roles for Instagram youth. And they are essentially for to find innovative ways to tackle appropriate content

standards via data analysis, experimentation, and statistical modeling.

The FTC needs experts that can understand and perform the same research, evaluate the work that Facebook and others are doing to perform the manipulation and the targeting in order to assess whether it is, in fact, harmful or problematic. And so I think in addition to authorities having experts in kids psychology, behavioral economics, design the UX and choice architecture, which is a lot of what this work is, is giving people, you know, manipulating people's choice, I think are going to be critical.

Senator BLUMENTHAL. Thank you very much for that response. I—my time has expired, so I would invite others to respond in writing, if you wish to do so. Very much appreciate all of you being here. Thank you.

The CHAIRWOMAN. Thank you, Senator Blumenthal. And thank you for your leadership at the Subcommittee level on this important issue and for your work with many of our colleagues on this and your letters. Thank you. That is continued focus on a very needed area.

I thank all of our witnesses today for testifying before the Committee. The hearing will remain open for a time period for members to submit questions. We ask you to respond to those in a timely fashion. And again, we appreciate the details and the information from the hearing today. We are adjourned.

[Whereupon, at 12:29 p.m., the hearing was adjourned.]

A P P E N D I X



September 29, 2021

Color Of Change Supports \$1 Billion in Funding for FTC Privacy Bureau

Color Of Change, the nation's largest online racial justice organization, strongly supports a provision of the House Energy and Commerce Committee's budget reconciliation bill that would allocate \$1 billion in funding for the Federal Trade Commission (FTC) privacy bureau. We urge lawmakers to advocate this funding and the inclusion of additional language that would designate funds for hiring staff with racial justice expertise.

To effectively serve Black communities, racial justice must be baked into the FTC's privacy policymaking and oversight. Discriminatory algorithms and data privacy affect the everyday lives of Black communities, including in education, employment, healthcare, and the criminal justice system.¹ Currently, data protection enforcers do not have the staff expertise to adequately incorporate racial justice and need additional funds to increase staff capacity. Funds must be explicitly set aside for staff with civil rights and racial justice expertise at the FTC, covering salaries and overhead costs.

¹ Colin Lecher and Maddy Varner, "NYC's School Algorithms Cement Segregation. This Data Shows How," *The City*, May 26, 2021, <https://www.thecity.nyc/2021/5/26/22453952/nyc-high-school-algorithms-segregation>; Miranda Bogen and Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn, December 2018, <https://www.upturn.org/reports/2018/hiring-algorithms/>; Jennifer Tsai, "Jordan Crowley Would Be in Line for a Kidney—if He Were Deemed White Enough," *Slate*, June 27, 2021, <https://slate.com/technology/2021/06/kidney-transplant-dialysis-race-adjustment.html>; Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, "Machine Bias," *ProPublica*, May 23, 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.



COLOR OF CHANGE
COLOROFCHANGE.ORG

We urge the Senate Commerce, Science, and Technology Committee to support the proposed \$1 billion in funding for the FTC privacy bureau in addition to language that would set aside funds for hiring staff with racial justice expertise. It is imperative that the full amount of funds is given to the FTC. Our communities need a fully equipped and well-resourced data regulator.

Please contact Gabrielle Rejouis (gabrielle.rejouis@colorofchange.org) with any questions.





1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

- **Permissible Uses**

The payments industry has a long history of fighting fraud and is constantly developing and deploying new technology to detect, deter, and eliminate fraud. New and enhanced technologies have amplified the payments industry's ability to offer new fraud solutions and strengthen our ongoing efforts. Any privacy or data protection standard should include provisions for permissible uses of data to prevent fraud and protect consumers.

- **Maximize Transparency**

Businesses must promote transparency with their customers as well as when engaging with regulators or other appropriate authorities. Regulators and government officials should be appropriately transparent about their objectives.

With respect to personal data, consumers should have reasonable access to clear and understandable statements about businesses practices and policies. Businesses should be transparent about the types of personal data collected, how the personal data will be used, and whether personal data may be disclosed or shared. Businesses should also provide clear privacy notices to consumers as well as appropriate procedures for individual control, including the opportunity to control data sharing.

- **Access to Data**

Individuals must have a reasonable right to access the personal information they have provided to a company and, where practical, the right to have that information corrected. Individuals should also have the ability to request the deletion of personally identifiable information provided to companies, unless there is a legitimate or legal obligation to retain that information.

- **Enforcement**

To protect consumer rights and provide responsibility, enforcement needs to be consistent and coordinated between the federal government and the state's regulatory body. Congress should encourage collaboration between the Federal Trade Commission ("FTC") and state attorneys general to enforce a national consumer privacy law. Strict coordination should be followed to avoid duplicate or conflicting enforcement actions. ETA believes the FTC should be granted targeted rulemaking authority and have civil penalty authority. However, a federal privacy law should not provide monetary relief in the form of a private right of action for privacy enforcement.

- **Maintaining Flexibility**

Technology that is involved in data processing evolves rapidly. A baseline law can provide clarity on achieving specific privacy principles; however, laws and regulations should undergo reviews and be flexible. A government should not mandate a specific technological solution or other instrument to implement consumer protections. Including a safe harbor within a federal privacy law would promote the development of adaptable, consumer-friendly privacy programs.

- **Global Leadership**



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

- **Permissible Uses**

The payments industry has a long history of fighting fraud and is constantly developing and deploying new technology to detect, deter, and eliminate fraud. New and enhanced technologies have amplified the payments industry's ability to offer new fraud solutions and strengthen our ongoing efforts. Any privacy or data protection standard should include provisions for permissible uses of data to prevent fraud and protect consumers.

- **Maximize Transparency**

Businesses must promote transparency with their customers as well as when engaging with regulators or other appropriate authorities. Regulators and government officials should be appropriately transparent about their objectives.

With respect to personal data, consumers should have reasonable access to clear and understandable statements about businesses practices and policies. Businesses should be transparent about the types of personal data collected, how the personal data will be used, and whether personal data may be disclosed or shared. Businesses should also provide clear privacy notices to consumers as well as appropriate procedures for individual control, including the opportunity to control data sharing.

- **Access to Data**

Individuals must have a reasonable right to access the personal information they have provided to a company and, where practical, the right to have that information corrected. Individuals should also have the ability to request the deletion of personally identifiable information provided to companies, unless there is a legitimate or legal obligation to retain that information.

- **Enforcement**

To protect consumer rights and provide responsibility, enforcement needs to be consistent and coordinated between the federal government and the state's regulatory body. Congress should encourage collaboration between the Federal Trade Commission ("FTC") and state attorneys general to enforce a national consumer privacy law. Strict coordination should be followed to avoid duplicate or conflicting enforcement actions. ETA believes the FTC should be granted targeted rulemaking authority and have civil penalty authority. However, a federal privacy law should not provide monetary relief in the form of a private right of action for privacy enforcement.

- **Maintaining Flexibility**

Technology that is involved in data processing evolves rapidly. A baseline law can provide clarity on achieving specific privacy principles; however, laws and regulations should undergo reviews and be flexible. A government should not mandate a specific technological solution or other instrument to implement consumer protections. Including a safe harbor within a federal privacy law would promote the development of adaptable, consumer-friendly privacy programs.

- **Global Leadership**



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

Congress should adopt policies that facilitate international electronic commerce and promote consumer privacy — both of which benefit consumers, economic growth, and trade. Burdensome international regulations hamper the growth of new businesses and create conflict of law between jurisdictions. Although the U.S. is uniquely positioned to benefit from the experience and regulatory proposals being adopted or considered by its international counterparts, having the U.S. establish a national privacy framework will facilitate an international data framework and reinforce U.S. leadership worldwide.

The payments industry never rests — we are working tirelessly to fight fraud and protect consumers by developing new tools to prevent or identify fraud data analysis as well as by frequently introducing new fraud-fighting solutions. Privacy laws should continue to recognize these goals and the important role the payments industry plays in combating fraud. By working together, lawmakers, regulators, and industry participants can protect consumers while providing them with access to the safest and most convenient payments system in the world.

ETA would like to thank the Committee for this opportunity to provide this statement for the record on this important topic. We appreciate your leadership on this important issue. If you have any questions, please feel free to contact me or ETA's Senior Vice President of Government Affairs, Scott Talbott, at stalbott@electran.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jeff Patchen', written over a light gray rectangular background.

Jeff Patchen
Senior Manager of Government Affairs
Electronic Transactions Association





¹ PRIVACY4CARS

www.Privacy4Cars.com

Comments To the U.S. Committee on Commerce, Science, and
Transportation on
“Protecting Consumer Privacy”
September 29th, 2021

Good morning Chair Cantwell, Ranking Member Wicker, and Members of the Commerce Committee. Privacy4Cars is pleased to present this statement to the Committee as it relates to your hearing on “Protecting Consumer Privacy.” Consumers here at home and abroad are demanding to know how and where their personal information is being gathered and stored. This Committee has been diligent in focusing on the protection, transparency, and use of consumers personal data and we commend the Committee for holding this public hearing.

Privacy4Cars was founded by a vehicle privacy and cybersecurity expert and is dedicated to providing simple and pragmatic privacy solutions to both consumers and businesses in the automotive industry. We have first-hand experience in the industry and we work with many industry players who are concerned with how modern vehicles retain Personal Information (PI) in In-Vehicle Infotainment Systems (IVIS) and Electronic and Telematics Control Units. As consumer safety advocates, we think it’s important to highlight and educate the public about the significant risks associated with leaving this data exposed and accessible to future vehicle owners, renters, and—potentially—those with nefarious intentions.

Vehicle manufacturers and service providers collect massive amounts of personal information through multiple sensors in the vehicle. Data collected includes precise geolocation, biometrics, detailed behavioral profiles of drivers and occupants—including minors—video and voice

¹ Our founder, Andrea Amico, has been heading the Privacy and Cybersecurity initiative at the International Automotive Remarketing Alliance (IARA, www.iara.biz), the industry association that reunites many of the leading players in the \$100 billion vehicle wholesaling industry in the US and Canada, including automotive OEMs, automotive finance companies as large as captives and national blue-chip banks to smaller regional auto leasing and lending companies, most of the main auto auctions, large fleet management and fleet companies such as rentals, vehicle repossession companies, dealers, and many other service providers. At IARA, Amico spearheaded the formation of a partnership with Auto-ISAC, the Information Sharing and Analysis Center, established by the automotive industry to address cybersecurity and privacy issues.

recordings, and even garage codes associated with home addresses. And when individuals sync their phones—a safety requirement in most states to enable hands-free controls—a treasure trove of personal information is sucked out from the phones into the vehicles, including contacts, call logs, text messages, and unique identifiers that make it easy to reassociate this data with specific individuals. In recent vehicles even more data may be downloaded, including social media account information, photos and files present on the phone, calendar entries, and financial and health information.

What should be of concern to this Committee and to policymakers of all political ideologies is the following jarring fact: more than 4 of 5 pre-owned cars sold in the U.S. *still contain the personal information* of previous owners, renters, or passengers! It is ludicrous to imagine individuals being willing to hand their cell phones—with all their personal data—over to strangers. Yet the driving public are often unaware that they are essentially doing the same thing every time they sell a vehicle, return a rental car, participate in a car sharing or subscription program, or on the occasion of when a vehicle is repossessed or in a total loss accident. The left-behind data is susceptible to easy discovery and manipulation. It is reported that thirty-six percent of automotive cybersecurity incidents are due to data and privacy breaches. (<https://upstream.auto/2021Report/>).²

Equally disturbing is the fact that personal information collected in vehicles through original equipment manufacturers (OEMs), aftermarket systems, or a variety of connected apps and other technologies flow beyond the auto industry, including law enforcement and government. Third parties and data brokers in the broad automotive ecosystem collect, share and sell this sensitive information without the knowledge of the affected individual. VICE recently reported that players in the vast vehicle data ecosystem—despite grand statements about being transparent and committed to consumer privacy—were, in fact, selling detailed geolocation data from which it was easy to reidentify individual consumers and reconstruct their daily movements. (<https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo>).

Those of us within this specialized industry have become embroiled in an intense, national debate over a fundamental question: Who owns this data? Most laypersons presented with this question answer simply, “We individuals do, of course!” Unfortunately, that’s often not the case.

² We launched Privacy4Cars and developed the first and only currently-accessible mobile process designed to erase PII from modern vehicles. To fulfill our social mission, we decided that our namesake Privacy4Cars app should be available as a free download for consumers on iOS and Android devices so they would have a tool to protect them against potential security breaches and theft of data.

Privacy policies and terms of service agreements are written by auto manufacturers and third party service providers to give themselves the unfettered legal ability to collect personal information—often with the right to use it in perpetuity and for whatever purpose they see fit.

Many vehicle telematics-based services advertise to consumers with phrases such as these: “Drive with confidence, knowing an Emergency-Certified Advisor is ready to help no matter what happens out on the road.” Or this: “We built our own telematics service platform from the ground up with a focus on resiliency, quality, and advanced safety features. When it comes to life saving services, there are no compromises.” In reality, when consumers sign up for these safety services, they likely do not realize they are also granting companies the right to use their information for personal profiling or advertising or that their personal data is being sold to insurance companies and data brokers.

Some service providers in the automotive industry are holding consumer safety features hostage until they’re given carte blanche to do whatever they want with the potential customer’s personal information. That’s wrong. Businesses should be prohibited from using consumer safety as a bargaining chip to convince Americans to turn over their personal data without allowing the individual to retain granular access control over how such sensitive data will be collected, stored, used, or shared.

Investing in consumer safety means acknowledging its relationship with data privacy and not giving away control of our personal information as a negotiating tactic. Consumers should have and deserve both. Here are some of our suggestions to better enhance and protect consumer privacy as it relates to automotive technology and safety:

- Prohibit a manufacturer or leasing agency from requesting a waiver of a vehicle user’s right to data or requiring such a waiver as a condition for purchasing, leasing, operating, or obtaining warranty repairs;
- Sensibly expand and redefine the concept of vehicle “owner.” As currently defined, owners can include corporations, financial institutions or entities that operate fleets which may use employees’ data for their own commercial interests;
- Require rental and carsharing companies to protect the personal information collected by vehicles and ensure that the data is not accessible to future vehicle users or that malicious spyware or “stalkerware” has been installed which may harm future renters. Similarly, auto insurance companies who end up owning a vehicle after it is deemed a total loss should have a duty and obligation to protect their policyholders’ data;
- Continue to build upon the good work of this Committee during consideration of the Driver Privacy Act of 2015 (S. Rept. 114-147) and expand the protections granted to the Electronic

Data Recorder in that bill to all computerized systems in vehicles, including the Electronic Control Units, In-Vehicle Infotainment Systems and Telematics Control Units—including aftermarket add-ons;

- Authorize the Federal Trade Commission or other appropriate governmental agencies to define, regulate, and—when appropriate—promote consumer advocates with specialized knowledge in the area of protecting the privacy and security of personal information captured and stored so that the data is not inadvertently or intentionally transmitted without the consent of the individual affected;³
- Ensure that the FTC receives adequate funding for the enforcement of data privacy rules.

Thank you for the opportunity to provide these comments. Privacy4Cars is committed to the important goal of ensuring that consumers are made fully aware of the extensive data that modern vehicles collect and how that information is being used. Moreover, we will continue to pursue policies so that consumers are given granular controls over their personal information so that no individual has to choose between privacy, security and safety in vehicles again.

We look forward to working with any and all stakeholders to address the challenges of consumer proprietary information in this exciting era of connected and autonomous vehicles. We welcome the opportunity to be a resource for this Committee in the areas of industry data, insights, or expertise.

Respectfully submitted,

Privacy4Cars
Mr. Andrea Amico
617.309.0937
info@privacy4cars.com

³ We increasingly receive requests from consumers asking for help with protecting the privacy and security of the personal information captured, stored, transmitted, shared, and sold. On many occasions we are asked for assistance in deleting same from a vehicle(s). We've also been asked to consult with a broad set of companies in the automotive space. It is our belief that consumer advocates with specialized knowledge can dramatically improve the ability of individuals to protect their personal information. In our experience, navigating the maze of vehicle data is extremely challenging since most companies who collect, share, and sell data are not vehicle manufacturers, but Business-to-Business (B2B) companies of whom most consumers have no knowledge. Consequently, even with broad consumer privacy rights, the non-transparency of the data markets severely limit an individual's ability to assert those rights.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RAY BEN LUJÁN TO
DAVID C. VLADECK

Question. As FTC Chair Lina Khan noted, the commodification of sensitive health information for behavioral ads or user analytics is a serious concern for user privacy. Question. How should Congress and the FTC protect sensitive health information from commodification? What additional safeguards are necessary to ensure this information is protected from data breaches or other nonconsensual distribution?

Answer. The question is a vexing one because it exposes the weakness in the statutory mandate of the Federal Trade Commission to safeguard consumer privacy. The FTC's consumer protection remit is to "prevent" "unfair and deceptive acts and practices in or affecting commerce." 15 U.S.C. §§ 45(a)(1) & (2). Congress has confined the FTC's "unfairness" mandate by requiring that an act be not only "unfair" to consumers, but also that the consumer could not "reasonably avoid[]" the unfair act. *Id.* at 45(n). Equally problematic, the FTC's deception authority depends on false, misleading, or omitted claims. Because consumers must "consent" to use websites, the harvesting of data is not necessarily deceptive. The FTC has long sought legislation to enable it to provide robust protection of sensitive data. After all, companies often use that data used for purposes that may be harmful to consumers. As I made clear in my written testimony, I urge Congress to enact more targeted general legislation giving the FTC the tools it needs to protect consumer privacy—tools the FTC has sought for several decades.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RAPHAEL WARNOCK TO
DAVID C. VLADECK

Question. Consumer Comprehension. Since the COVID-19 pandemic, we have all learned how to use a lot of new online tools—whether for work, school, or telehealth. And most of the time that we log into these new applications, we're given a 10 or 20 page "privacy policy" that is full of complicated legal language and jargon, and many consumers are left confused about what their rights are and what they have signed away. Question. How can Congress and the FTC make it easier for consumers—especially those with lower levels of digital literacy—to understand and control how their data is used and collected?

Answer. At least since my tenure at the FTC, starting in 2009, the Commission has railed at the "privacy policies" as little more than obfuscation for consumers. Consumers have to endure to try to understand the basic questions about what consumer data is being harvested, by what companies, and for what purposes? What are companies doing with that data? Is the data being used for targeted ads? Are companies using your personal information to make ads even more effective? Are the companies engaged in geolocation tracking? Are companies selling your data to other companies? And if so, to what companies, and for what purposes? I could go on. But you see my point. Lawyers write privacy policies to provide enough information so that the policy is not deceptive, but no more information than is absolutely necessary.

My view is that the term "privacy policy" is a gross misnomer. These policies are not "privacy policies" at all. Most of these policies deal with data-acquisition and use; not privacy. In truth, they are data use policies, which are invariably non-negotiable. Consumers use websites and apps on a take-it-or-leave-it basis, and consumers rarely leave it because they need to be able to engage in our digital economy.

As with the prior question, the FTC cannot change the *status quo* without clearer, more powerful, and more targeted tools to protect consumer privacy on line. This question, like the one submitted by Senator Luján, goes to the heart of the FTC's limited ability to protect consumer privacy. I urge the Committee to continue to develop legislation aimed at addressing these and other issues relating to online privacy.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO
DAVID C. VLADECK

Question. Do you believe that a single national privacy standard should provide consumers with more control of their data and how do we ensure that data is protected?

Answer. Yes, I believe that it is time for Congress to enact comprehensive privacy legislation that provides consumers far more control of their data than they can exercise at the present. The FTC's existing mandate permits the Commission to reign

in practices that are deceptive and unfair, but that mandate is insufficient to provide robust privacy protection, especially when services are offered on a take-it-or-leave-it basis.

Equally problematic is that all too often companies do not make sufficient investment in safeguarding data, including data that has commercial value (like payment card information) or is sensitive for other reasons. The FTC has brought dozens of enforcement cases against companies that have failed to take reasonable measures to secure sensitive information, but apart from bringing an enforcement action and getting the company under order, there is no redress or penalty for first violations under the Federal Trade Commission Act. As a result, deterrence kicks in only *after* a company has experienced a breach due to unduly lax security. Congress needs to authorize the FTC to impose civil penalties on first offenders, or else the status quo will remain in place and companies will get at least one free bite at the apple.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARSHA BLACKBURN TO
DAVID C. VLADECK

Question. Over the past few years, developers have been creating new financial services apps directed towards children. As more parents sign their kids up for these apps, it raises questions about what kinds of data they are collecting and how they use it.

Do you share these concerns and what steps do you think we should take to get a better handle on this issue?

Answer. I share your concerns, and worry that parents might sign up their children for these apps without any understanding about what data the companies are collecting and how that data is being used. Of course Congress, with its broad investigatory powers, could undertake an investigation. But so too could the FTC. But your question underscores the need to provide more resources to the FTC, which is severely under-staffed and under-funded. Until the FTC is adequately resourced, it will necessarily engage in triage, leaving some important matters unaddressed, or deferred. With needed resources, the FTC could undertake an investigation of these apps to answer the questions you pose about data harvesting and use. The FTC could do so by investigating a few companies offering these apps, or, if appropriate, through a broader industry study under the FTC's authority under 6(b) of the FTC Act. In that event, the FTC would then issue a report addressing the questions you posed, and thus give parents the information they need to make an informed decision.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BEN RAY LUJÁN TO
MAUREEN K. OHLHAUSEN

I'm especially concerned by websites collecting personal information when a user hasn't entered into any agreement or been presented with information on how that collected information may be used or sold.

Question. How should the FTC and Congress protect the data of individuals who have never signed up for an account or signed terms of service?

Answer. Section 5 of the FTC Act gives the FTC authority to prevent "unfair" acts or practices that cause or are likely to cause substantial harm to consumers that consumers cannot reasonably avoid and that are not outweighed by countervailing benefits to competition or consumers. Using this authority, the FTC has brought enforcement actions in situations where websites that do not have relationships with individual consumers collect their personal information and use it in a way that harms them or collect consumers' sensitive personal information without their consent.

While the FTC has used its limited authority in these situations, Congress can provide even greater protections to consumers by enacting comprehensive, technology neutral, national privacy legislation that provides clear protections for consumers, articulates specific limits on companies' ability to collect, use, and share sensitive personal information, and grants the FTC the resources and explicit authority necessary to enforce a new law.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RAPHAEL WARNOCK TO
MAUREEN K. OHLHAUSEN

Consumer Comprehension. Since the COVID-19 pandemic, we have all learned how to use a lot of new online tools—whether for work, school, or telehealth. And

most of the time that we log into these new applications, we're given a 10 or 20 page "privacy policy" that is full of complicated legal language and jargon, and many consumers are left confused about what their rights are and what they have signed away.

Question. How can Congress and the FTC make it easier for consumers—especially those with lower levels of digital literacy—to understand and control how their data is used and collected?

Answer. Due to the COVID-19 pandemic, we have seen a rapid shift to online work and learning, which makes even more apparent the need for comprehensive privacy legislation that makes privacy protections uniform, clear, and transparent. Congress should enact Federal privacy legislation that includes several key attributes that will help make privacy policies clearer and simpler for all Americans. First, legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. Second, it should ensure strong enforcement that protects consumer information that could result in harm if disclosed or misused, while also allowing companies to provide and develop innovative products and services that consumers want. Third, it should provide consumers clarity and visibility into companies' data collection, use, and sharing practices, as well as easily understandable choices regarding these practices, calibrated to the sensitivity of that data. Fourth, legislation should be more comprehensive than current state laws, such as the CCPA, addressing more elements of the data cycle. Fifth, Federal privacy legislation should be enforced by the FTC, which has the experience and skill to meaningfully enforce a new law's protections, supplemented by state attorneys general.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
MAUREEN K. OHLHAUSEN

Question 1. Do you believe a single national privacy standard should provide consumers with more control of their data and how do we ensure that data is protected?

Answer. Yes, I believe a single national privacy law would provide consistent enhanced protections to consumers throughout the United States, which means they would have this increased control regardless of where they live, work, or visit. Congress should ensure that a single national privacy law includes strong privacy protections.

Question 2. I believe it is Congress' responsibility to take action on privacy legislation rather than punting it to the FTC. Can you talk about some of the challenges the FTC would have by conducting a non-preemptive rulemaking to address privacy concerns?

Answer. I have three primary concerns about a non-preemptive FTC rulemaking. First, given the scope of the FTC's current statutory authority, an FTC rulemaking could not be as comprehensive as legislation. Second, under the FTC's Magnuson-Moss rulemaking requirements, a general privacy rulemaking involves a cumbersome process and is time-consuming. Third, a non-preemptive rulemaking could cause confusion and uncertainty about what requirements apply in a particular state and create regulatory complexity that hurts small business.

Question 3. The PACT Act, Section 230 legislation I introduced with Senator Schatz would, among other things, provide that the immunity provided by Section 230 does not apply to civil enforcement actions brought by the Federal government.

Do you believe that by reforming Section 230 to ensure that the immunity provided by Section 230 does not apply to civil enforcement actions brought by the Federal government, such as the FTC, would benefit consumers?

Answer. Unfortunately, Section 230 is beyond my areas of expertise.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO
MAUREEN K. OHLHAUSEN

Question 1. I share the concerns you highlighted in your testimony about the FTC moving forward with a privacy rulemaking without a Federal law enacted by Congress to set the guidelines for consumers and businesses. I introduced the Browser Act (one of the first bipartisan privacy bills in Congress), as well as the Safe Data Act with Senator Wicker, and am fully committed to getting a Federal privacy law across the finish line. So I'm understandably wary of actions the FTC has taken to short circuit its rulemaking procedures in order to plow ahead with a privacy rulemaking.

Can you walk us through some of the problems here?
Is this a way to enact policies that might not get bipartisan support in Congress—or even things the FTC might not be legally authorized to do?

Answer. I have three primary concerns about an FTC general privacy rulemaking. First, given the scope of the FTC's current statutory authority, an FTC rulemaking could not be as comprehensive as legislation. Second, under the FTC's Magnuson-Moss rulemaking requirements, a general privacy rulemaking involves a cumbersome process and is time-consuming. Third, a non-preemptive rulemaking could cause confusion and uncertainty about what requirements apply in a particular state, and create regulatory complexity that hurts small business.

Question 2. When you were an FTC Commissioner, you played a key role in negotiating the privacy shield for international data transfers after the “safe harbor” provisions were struck down.

How was the U.S. able to come to a deal with the EU last time, and why are we struggling to provide this certainty to businesses and consumers now?

Answer. While we reached an agreement on the Privacy Shield last time, the European court eventually found it was not sufficient. Having a comprehensive Federal law may help support a lasting EU determination that our privacy law is adequate under EU law, thereby providing greater certainty to businesses and consumers.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BEN RAY LUJÁN TO
ASHKAN SOLTANI

NOTE: The following responses are provided in my personal capacity and do not reflect or represent the views of any employer, past or present.

Question. In your testimony, you refer to the need to enable to FTC to better compete and retain *talented* individuals with relevant skills and experience. What reforms do you believe would be most impactful in making the Commission more competitive when hiring for top-level talent?

Answer. As I noted in my testimony, based on my experiences as Chief Technologist of the Federal Trade Commission (FTC), the FTC needs more resources to hire technologists and to attract top talent. I appreciate Senator Lujan's continued commitment to helping to ensure that the FTC has the resources it needs to build its technology staff. For example, Senator Lujan's Federal Trade Commission Technologists Act, which was introduced in the House of Representatives by Rep. McNerney of California, provides funding to create a separate Office of Technology in the FTC, staffed with at least 25 technologists. This would be an excellent first step in building the FTC's capacity to police unfair and deceptive practices related to privacy and data security.

Senator Lujan's bill is important not only because it would allow the FTC to hire more technologists, but because the creation of a separate office for technologists would allow them to more effectively support all FTC divisions. Technologist support is important not only for the Division of Privacy and Identity Protection (DPIP), which initiates investigations, but for the enforcement team as well, which is a separate division that oversees compliance with FTC orders across all divisions. Technologist support is also needed at the Bureau of Competition, since technology and data pervade nearly every case that comes before the Commission. Housing the technologists in a separate office will make it more likely that they will be able to provide support across the Commission.

Of course, it's also important to attract and retain top talent. Top technologists would likely make far less in the public sector than they could in the private sector. At minimum, the FTC should be prepared to match candidates' existing salaries.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RAPHAEL WARNOCK TO
ASHKAN SOLTANI

Consumer Comprehension. Since the COVID-19 pandemic, we have all learned how to use a lot of new online tools—whether for work, school, or telehealth. And most of the time that we log into these new applications, we're given a 10 or 20 page “privacy policy” that is full of complicated legal language and jargon, and many consumers are left confused about what their rights are and what they have signed away.

Question. How can Congress and the FTC make it easier for consumers—especially those with lower levels of digital literacy—to understand and control how their data is used and collected?

Answer. I can certainly sympathize with consumers who are frustrated by incomprehensible privacy policies. Businesses should be required to clearly outline their data practices—not only to inform consumers, but so that enforcement authorities can hold businesses accountable for wrongdoing. California has been a leader in this space, and as early as 2003, adopted the California Online Privacy Protection Act (CalOPPA), becoming the first state to require businesses to outline their data practices in a public privacy policy.

In addition, the California Consumer Privacy Act of 2018, as amended by Proposition 24, the California Privacy Rights Act of 2020 (CCPA), takes steps to make privacy policies accessible for the public. Under the CCPA, California consumers have the right to know what personal information a business has collected about them and how it is used and shared. The California law requires businesses to inform consumers of the categories of information it has collected, the categories of sources from which it was collected, the business or commercial purpose for collecting, selling, or sharing personal information, and the categories of third parties to whom the business discloses personal information.

Importantly, the CCPA regulations require businesses to ensure that the notices and information that businesses are required to provide, are presented in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer. This performance-based approach clarifies that disclosures and communications must be designed and presented in a way that is easy to read and understandable by consumers, including those with disabilities. And the regulations use the language of “reasonably accessible to consumers with disabilities” to acknowledge that the definition of disabilities may be broad, and thus, the business’s obligations are tied to a generally recognized industry standard such as the Web Content Accessibility Guidelines.¹

In addition, businesses are currently required by CCPA regulation to honor browser privacy signals as a global opt out of sale, so that consumers can exercise their privacy preferences with covered businesses in a single step,² rather than needing to seek out cumbersome settings with every business they interact with. These provisions together help make the CCPA workable for consumers of all levels of literacy and sophistication.

Lastly, the CCPA is not only designed to make it easy for consumers to *exercise* their rights, it also provides protections beyond just “notice and choice” through its data minimization and purpose limitation provisions. The CCPA, as amended by the CPRA, introduces data minimization and purpose limitation provisions that put limits on the collection, use, retention, and disclosure of personal information in the first place, so that consumer privacy is protected by default.³ These provisions are described in more detail in the next response.

Data Minimization Requirements. In 2018, the Supreme Court held that under the Fourth Amendment, law enforcement officers must apply for a warrant to obtain cell-site location data from wireless carriers. That is because location data can reveal intimate details about our lives. Recently, however, we have seen reports that law enforcement agencies are obtaining consumers’ location data through commercial vendors, bypassing these Constitutional protections. One way to curb these practices would be to require that technology companies employ data minimization practices, so that data could only be stored for specific purposes.

Question. Do you believe data minimization procedures would help protect consumer privacy?

Answer. Yes. Data minimization and purpose limitation provisions are increasingly common in privacy legislation. These provisions typically prohibit unnecessary collection, use, retention, and disclosure of personal information—and in so doing, enable consumers to use online products and services safely, without having to take additional steps to protect their privacy. Data minimization and purpose limitation language was added to the California Consumer Privacy Act by Proposition 24, and uses language consistent with language in Europe’s General Data Protection Regulation (GDPR), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and Connecticut’s new privacy law—highlighting its increased currency. The CCPA as amended by Proposition 24 states, “A business’s collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the con-

¹ Cal. Code Regs. tit. 11 § 7011

² Cal. Code Regs. tit. 11 § 7026

³ Civil Code § 1798.100(c).

text in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.”⁴

In addition, two new California laws have placed new data minimization requirements on certain covered businesses. For example, SB 1172, the Student Test Taker Privacy Protection Act, provides that, subject to certain exemptions, “a business providing proctoring services in an educational setting shall collect, use, retain, and disclose only the personal information strictly necessary to provide those services.”⁵

Similarly, AB 2273, the California Age-Appropriate Design Code, has several provisions that minimize data processing. For example, it provides that, subject to certain exemptions, a covered business may not collect, share, sell, or retain any personal information that is not necessary to provide a product, service, or feature with which a child is actively and knowingly engaged, unless the business can demonstrate a compelling reason that such processing is in the best interests of children likely to access the product, service, or feature. Additionally, the law provides that businesses may not collect, sell, or share precise geolocation information of children by default, unless the collection is strictly necessary to provide the requested product, service, or feature, and only then for the limited time that such collection is necessary to provide it.⁶

Both measures, like the CCPA as amended, limit the personal information businesses can collect and use to what the average consumer would expect in that situation *without* having to obtain explicit consent.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RAPHAEL WARNOCK TO
MORGAN REED

Consumer Comprehension. Since the COVID-19 pandemic, we have all learned how to use a lot of new online tools—whether for work, school, or telehealth. And most of the time that we log into these new applications, we’re given a 10 or 20 page “privacy policy” that is full of complicated legal language and jargon, and many consumers are left confused about what their rights are and what they have signed away.

Question. How can Congress and the FTC make it easier for consumers—especially those with lower levels of digital literacy—to understand and control how their data is used and collected?

Answer. ACT | The App Association recognizes that the modern notice and consent model is not always a sufficient means of communicating privacy expectations or establishing a relationship of trust. Consent often fails to contemplate dynamic uses of data and does not encapsulate consumers’ future expectations given the passage of time or changing contexts. We believe Congress has the best position, through the framework of a Federal privacy law, to retool the consent model so that it centers on consumer experience while preserving the ability for small innovators to compete and develop better privacy practices and communication methods.

Our members currently leverage several promising efforts developed at the platform level to enhance consumer understanding and control over their data outside of the traditional privacy policy paradigm. For example, Apple recently introduced privacy “nutrition” labels that allow app developers to give users a more intuitive sense of the app’s privacy policies, allowing good actors to easily demonstrate their commitment to responsible privacy stewardship. The nutrition label surfaces key information for users, saving them from having to dig through the entire privacy policy. Apple’s new App Tracking Transparency tool also provides an easy and efficient way for users to opt-out of unwanted tracking that follows them outside of the app onto websites or even other third-party apps. Proposals introduced by the Chair and Ranking Member of the committee, including the SAFE DATA Act and Consumer Online Privacy Rights Act (COPRA), align with those advancements by requiring consumer friendly opt-out rights for non-sensitive personal information. As Congress and the Federal Trade Commission debate future policymaking on privacy issues, they should consider how they can encourage and incentivize further development of such privacy-enhancing technologies. At the same time, Congress should also reject proposals like the American Innovation and Choice Act (S. 2992), which would expand the scope of antitrust law in ways that presume the illegality of these platform level privacy controls.

⁴ Civil Code § 1798.100(c).

⁵ SB 1172, The Student Test Taker Privacy Protection Act (2022), https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB1172.

⁶ AB 2273, The California Age-Appropriate Design Code (2022), https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB2273.

Another consideration is that our Nation's current patchwork approach to privacy, with incongruous sectoral privacy laws (including the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act) and growing differences among the states, greatly contributes to consumer confusion. A Federal privacy law that creates strong consumer rights will raise the baseline of protection, ensuring that no matter where in the country a person lives, they enjoy certain protections. In particular, a Federal law should empower consumers to exert more control over their personal information, including the rights to access, correction, and deletion of such information. Sensitive personal information should also be subject to some limits on processing activities that pose too great a risk to consumers, which is not outweighed by countervailing benefits.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
MORGAN REED

Question 1. Do you believe a single national privacy standard should provide consumers with more control of their data and how do we ensure that data is protected?

Answer. Yes. Let me break this question down into its constituent parts:

1. A single, national privacy standard. Ensuring that a general, Federal consumer privacy law is the law of the land across all states is critical to achieving Congress' goals in this space and is the best outcome for App Association members and your constituents for a few reasons:
 - a. *Compliance.* Our member companies may be the smallest software and connected device makers, but they are not afraid of complying with strong privacy laws. Yet, what separates them from much larger companies is that they have a lower tolerance for compliance with slightly differing regimes across states, whether those differences directly conflict or not. This is especially true if complying with different obligations requires substantial expenditures that do not result in greater consumer protection. Compliance for compliance's sake imposes needless costs on small firms in the app economy and is an inefficient way of changing behavior, which we know is a major aim of privacy legislation. In fact, the lack of a single set of Federal rules has led small companies not to invest, in large part due to uncertainty about how states will legislate on privacy. As our member company Walker Tracker has shared, they mainly ruled out smaller clients and smaller contracts due to uncertainty about privacy compliance costs in the next year. These are tangible costs that affect your constituents and our member companies.
 - b. *Consumer benefit.* Although states actively compete with each other to provide better (a subjective concept) privacy protections than their peers, these differing regimes may actually be unhelpful for consumers, especially in today's mobile environment. A major feature of most of these state proposals and new laws is a set of consumer rights to access, correct, and delete information about themselves held by covered companies. To the extent that the dimensions of these rights and the process used to effectuate them differ, consumers are likely to be confused about how it is supposed to work. Each state might carefully design the process they envision to be user-friendly and therefore effective protections, but a South Dakota resident might think California's privacy law applies to her, but she would be wrong. If South Dakota enacts a general privacy law with consumer rights, covering South Dakota residents, she would be able to exercise those rights—but how do they differ from California's process, which the press continues to cover much more extensively? Is it even worth trying to make use of them when the company actually calibrated its compliance program to California's law and has not yet figured out how to deal with South Dakota's? This scenario does not help the South Dakota resident much.
 - c. *Global Competitiveness.* Europe's General Data Protection Regulation (GDPR), despite its flaws, is mainly preemptive of analogous Member State privacy laws. Through a single set of privacy laws that govern the continent, the European Union (EU) made a statement to its global trading partners and others that it is both serious about privacy and that processing data on EU subjects would involve compliance with a single set of laws (albeit enforced differently by Member State data protection authorities). Placing American companies at a relative disadvantage by saddling them with anywhere from three to 50 different privacy regimes across the

states hurts our privacy profile in the trade context and also undermines global competitiveness of U.S. based industries.

2. Putting consumers more in control of their data. A Federal law should empower consumers to exert more control over their personal information, including the rights to access, correction, and deletion of such information. Sensitive personal information should also be subject to some limits on processing activities that pose too great a risk to consumers, which is not outweighed by countervailing benefits.
3. Better data protection. Federal privacy legislation should include a data security requirement. We support the SAFE DATA Act (S. 2499), a version of which you co-authored last year. This Congress' version includes a data security requirement at Section 203, which strikes a good balance. Specifically, it requires covered entities to maintain reasonable a) administrative, b) technical, and c) physical data security policies and practices to protect against risks to the confidentiality, security, and integrity of covered data. Notably, the requirements are scalable insofar as they must be appropriate to the size and complexity of the covered entity; the nature and scope of the covered entity's collection or processing of covered data; the volume and nature of the covered data; and the costs of available tools to improve security and reduce vulnerabilities. Section 203 also provides that the required data security practices take baseline measures to address security threats, and that they are designed to: identify and assess vulnerabilities; take reasonable preventative and corrective action to address known vulnerabilities; and detect, respond to, and recover from security incidents. These are robust requirements that exceed most state law requirements and would better protect consumers from the threat of data security incidents, while allowing flexibility for smaller companies to comply and compete.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO
MORGAN REED

Question 1. You represent many members of the app ecosystem.

Are any of your members engaged in marketing financial service apps to kids? If so, what are they doing to protect kids' personal and financial data?

Answer. REGO Payment Architectures offers an app available now on the App Store, Mazoola, marketed to parents to enable their kids to engage in limited digital transactions, with parental control and guidance. As a financial services company, Mazoola is subject to the Gramm-Leach-Bliley Act (GLBA)—but is not necessarily required to comply with the Children's Online Privacy Protection Act (COPPA). Nonetheless, Mazoola complies with both GLBA and COPPA and requires parents to provide verifiable parental consent (VPC) before they collect any data pertaining to children under the age of 13. By complying with both regimes, Mazoola observes strict rules around consent for collection of data found in COPPA rules and also complies with the robust Federal Trade Commission (FTC) Safeguards Rule under GLBA. The FTC is actively reviewing the Safeguards Rule and has proposed updates including a requirement for financial institutions to use strong encryption to protect financial information, including when it pertains to children.

Your question also raises a concern we have with how the FTC tries to address privacy gaps in the absence of Federal privacy legislation. For example, the FTC issued a policy statement on September 15, 2021, indicating its intention to enforce its health breach notification rule in situations that do not involve a data breach. Specifically, the statement articulates the FTC's position that the rule applies when companies engage in "sharing of covered information without an individual's authorization."¹ Sharing of information on purpose with a third party without proper consent or authorization, or in a manner that disrespects the context and expectations of a consumer, is a privacy issue, not a data breach. The FTC's statement, therefore, is concerning and is both an inadequate and a confusing fix in the absence of Congress providing authority for it to stop and prevent privacy harms. A similar situation could arise in the context of financial services, where a gap arguably exists in the applicability of COPPA to financial institutions. Leaving gaps creates risks for consumers and businesses, especially with the aggressive posture of the current

¹ Fed. Trade Comm'n, Statement of the Comm'n on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

FTC, and that further underscores the need for Congress to enact a single, Federal set of rules on privacy that address these gaps.

Question 2. In your testimony, you mention the Open App Markets Act, my bill with Senators Blumenthal and Klobuchar, and suggest that legislation like ours would open the door to malware and privacy harms. While I fully appreciate the need to ensure privacy and security on all of our devices, I also find it interesting that a senior engineer at Apple was quoted as saying its app store security now is like “bringing a plastic butter knife to a gun fight.” It’s also curious that other decisions to exclude apps, like the Navalny opposition app in Russia, are made without any claims about security or privacy.

It seems like these companies should be able to protect user privacy without using it as a smokescreen to keep out competition or to justify political decisions—do you have ideas on how to do that?

Answer. While Apple’s security capabilities are not perfect—and perfect security really does not exist—its track record is demonstrably better than other software platforms in the market. For example, over the past four years, Android devices were found to have 15 to 47 times more malware infections (the variation attributable to the variety of different kinds of Android devices) than iOS devices.² This is no accident. Even if there is something to what the senior engineer who called out Apple’s security practices said, the policy of prohibiting sideloading is not a technical measure but a structural control to avoid risk surfaces altogether. While some critics suggest software platforms need not prohibit sideloading to maintain a secure environment, experience shows the opposite is true. Disallowing sideloading—or in Android’s case, requiring consumers to overcome default settings to allow sideloading—helps keep both marketplaces safer and more trusted than they would be otherwise. And that focus on security creates the necessary conditions for App Association members to succeed.

App store decisions with respect to allowing or disallowing apps on their platforms are also imperfect. Political pressure to allow or disallow apps is unfortunately common and our member companies have concerns if approval or removal decisions appear to have political motivations, especially if they might be applied differently from how they would be applied to smaller companies that do not appear in political headlines. However, App Association members currently have a choice between distinct software platforms through which to offer their products and services. Even though they are not happy with every app review decision, they are not asking government officials or a Federal regulation to supplant app store determinations, and if that were to happen, undue political influence on app removal or approval decisions could worsen. They would prefer the market for developer services to drive those results.

A Federal privacy regime, similar to what you proposed with the SAFE DATA Act, would help ensure that privacy is not a smokescreen for anticompetitive conduct in a few ways. First, SAFE DATA includes a right to data portability that requires covered entities to provide certain data of an individual in a portable, structured, and machine-readable format that is not subject to licensing restrictions. This provision would help ensure that large social media platforms, for example, are not thwarting a consumer’s ability to port their own data to a new service with obstacles that have little privacy value and an anticompetitive purpose. Second, it is important that strong privacy and data security requirements accompany any portability or interoperability mandate and this Congress’ SAFE DATA Act checks both of those boxes. Portability and interoperability should not flip the FTC’s own mantra of “privacy by design” to a new ethos of “access by design.” Lastly, a Federal privacy regime would establish a common understanding of privacy requirements, definitions, and obligations across the broad swath of the economy not otherwise subject to Health Insurance Portability and Accountability Act (HIPAA), GLBA, or similar industry-specific laws. Such a regime would help policymakers and enforcers distinguish legitimate privacy measures the law requires or condones against those that harm consumers and competition more than they benefit the market.



²Apple Inc., Building a Trusted Ecosystem for Millions of Apps: A Threat Analysis of Sideloading (Oct. 2021), available at https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf.